



Technical Report

Deploying VMware vCenter Site Recovery Manager 4 with NetApp FAS/V-Series Storage Systems

Larry Touchette, Julian Cates, NetApp
February 2012 | TR-3671 | Version 1.4

DEPLOYING VMWARE VCENTER SITE RECOVERY MANAGER 4 WITH NETAPP FAS/V-SERIES STORAGE SYSTEMS

The following document provides information regarding the deployment of VMware vCenter Site Recovery Manager version 4, with NetApp® storage systems running NetApp Data ONTAP operating in 7-Mode. The purpose of this document is to set appropriate expectations, for customers and NetApp employees, with respect to supported configuration, best practices, and methods for a successful implementation.

TABLE OF CONTENTS

1	INTRODUCTION	3
1.1	INTENDED AUDIENCE	3
2	OVERVIEW OF A DISASTER RECOVERY SOLUTION.....	3
2.1	A TRADITIONAL DR SCENARIO	4
3	BENEFITS OF IMPLEMENTING SRM WITH NETAPP	4
3.1	VMWARE VCENTER SITE RECOVERY MANAGER.....	4
3.2	NETAPP SNAPMIRROR	5
3.3	NETAPP FLEXCLONE.....	6
3.4	UNIFIED ARCHITECTURE FLEXIBILITY	6
3.5	NEW FEATURES IN SRM FOR VSPHERE.....	6
3.6	NEW FEATURES IN THE NETAPP SRM ADAPTER FOR VSPHERE.....	6
4	ENVIRONMENT DESIGNS	7
4.1	ENVIRONMENT DESCRIPTION	7
4.2	IP ADDRESS CHANGES	8
4.3	NFS STORAGE CONNECTIVITY	8
4.4	DR TESTING NETWORK CONSIDERATIONS	9
4.5	ACTIVE DIRECTORY SERVICES CONSIDERATIONS.....	9
5	REQUIREMENTS.....	10
5.1	SUPPORTED STORAGE PROTOCOLS	10
5.2	SRM/SRA VERSION DEPENDENCIES	10
5.3	SRA AND DATA ONTAP VERSION DEPENDENCIES.....	11
5.4	SUPPORTED REPLICATION TECHNOLOGIES.....	11
5.5	SUPPORTED REPLICATION LAYOUTS	11
5.6	MULTISTORE VFILER REQUIREMENTS	13
5.7	GENERAL ENVIRONMENT REQUIREMENTS	14
6	INSTALLATION AND CONFIGURATION	15
6.1	OVERVIEW	15
6.2	PAIRING PRIMARY AND DR SITES	15
6.3	USING HTTPS/SSL TO CONNECT TO THE NETAPP CONTROLLERS	16
6.4	CONFIGURING ACCESS TO THE NETAPP CONTROLLERS	16
6.5	CONFIGURING INVENTORY PREFERENCES.....	19
6.6	BUILDING A PROTECTION GROUP	20
6.7	CREATING A RECOVERY PLAN.....	22
7	EXECUTING RECOVERY PLAN: TEST MODE	24
8	EXECUTING RECOVERY PLAN: TRUE DR SCENARIO	26

8.1	REQUIREMENTS AND ASSUMPTIONS	26
8.2	EXECUTING THE RECOVERY PLAN	27
9	RESYNC AFTER RECOVERY	29
9.1	REQUIREMENTS AND ASSUMPTIONS	29
9.2	RESYNCING: PRIMARY STORAGE RECOVERED	30
9.3	RESYNCING: PRIMARY STORAGE LOST.....	33
9.4	REESTABLISHING PRIMARY-TO-DR REPLICATION.....	34
10	BEST PRACTICES	34
11	KNOWN BEHAVIORS	35
12	REFERENCE MATERIALS	37
	APPENDIX A: VMS WITH NONREPLICATED TRANSIENT DATA	39
	PROTECTING VMS ON ESX HOSTS WITH NONREPLICATED SWAPFILES	39
	PROTECTING VMS WITH NONREPLICATED WINDOWS PAGE FILES	41
	APPENDIX B: NON-QUIESCED SMVI SNAPSHOT RECOVERY.....	45
	NON-QUIESCED SMVI SNAPSHOT RECOVERY CONFIGURATION RULES	45
	USING THE NON-QUIESCED SMVI SNAPSHOT RECOVER FEATURE.....	45

1 INTRODUCTION

This document is a detailed, in-depth discussion around how to implement VMware® vCenter Site Recovery Manager (SRM) with NetApp FAS/V-Series storage systems. After reading this document the reader will be able to install and configure SRM and understand how to run a disaster recovery (DR) plan or DR test. In addition, the reader will have a conceptual understanding of what is required in a true DR scenario, which is much broader than just failing over the virtual infrastructure and storage environment.

1.1 INTENDED AUDIENCE

This document is intended for anyone who wants to install/use SRM in a NetApp storage environment. This document assumes that the user has experience with both NetApp and VMware products, specifically SnapMirror® and VMware vCenter Server. In addition, the reader should have knowledge of DR solutions and the workflow required in a DR scenario.

2 OVERVIEW OF A DISASTER RECOVERY SOLUTION

To architect a DR solution, you should keep the following factors in mind:

- Recovery time objective (RTO): RTO refers to how quickly a business can recover from the disaster, or specifically how long does it take to execute the recovery process, making business services available again.
- Recovery point objective (RPO): RPO refers to how far back in time the data in the environment will be once it has been made available.
- Scalability and adaptability in a growing environment.

The ideal solution will have both a low RPO (minutes) and RTO (minutes to hours). One factor that is often overlooked in a DR solution is the ability to test the DR solution in an efficient manner. In physical environments, DR testing can take many hours or even days and require that replication between sites be stopped while testing is performed.

2.1 A TRADITIONAL DR SCENARIO

When failing over business operations to recover from a disaster, there are several steps that are manual, lengthy, and complex. Often custom scripts are written and utilized to simplify some of these processes. However, these processes can affect the real RTO that any DR solution can deliver. Consider this simplified outline of the flow of a traditional disaster recovery scenario:

1. A disaster recovery solution was previously implemented, and replication has been occurring.
2. A disaster occurs that requires a failover to the DR site. This might be a lengthy power outage, which is too long for the business to withstand without failing over, or a more unfortunate disaster, causing the loss of data and/or equipment at the primary site.
3. The DR team takes necessary steps to confirm the disaster and decide to fail over business operations to the DR site.
4. Assuming all has been well with the replication of the data, the current state of the DR site, and that prior testing had been done to confirm these facts, then:
 - a. The replicated storage must be presented to the ESX hosts at the DR site.
 - b. The ESX hosts must be attached to the storage.
 - c. The virtual machines must be added to the inventory of the ESX hosts.
 - d. If the DR site is on a different network segment than the primary site, then each virtual machine might need to be reconfigured for the new network.
 - e. Make sure that the environment is brought up properly, with certain systems and services being made available in the proper order.
5. After the DR environment is ready, business can continue in whatever capacity is supported by the equipment at the DR site.
6. At some point, the primary site will be made available again, or lost equipment will be replaced.
7. Changes that had been applied to data while the DR site was supporting business will need to be replicated back to the primary site. Replication must be reversed to accomplish this.
8. The processes that took place in step 4 must now be performed again, this time within a controlled outage window, to fail over the environment back to the primary site. Depending on how soon after the original disaster event the DR team was able to engage, this process might take nearly as long as recovering from the DR event.
9. After the primary environment is recovered, replication must be established in the original direction from the primary site to the DR site.
10. Testing is done again, to make sure that the environment is ready for a future disaster. Any time testing is performed; the process described in step 4 must be completed.

As mentioned earlier, a DR process can be lengthy, complex, and prone to human error. These factors carry risk, which is amplified by the fact that the process will need to be performed again to recover operations back to the primary site when it is made available. A DR solution is an important insurance policy for any business. Periodic testing of the DR plan is a must if the solution is to be relied on. Due to physical environment limitations and the difficulty of performing DR testing, most environments are only able to do so a few times a year at most, and some not at all in a realistic manner.

3 BENEFITS OF IMPLEMENTING SRM WITH NETAPP

Implementing a virtualized environment using VMware vCenter Site Recovery Manager on NetApp storage provides the infrastructure for unique opportunities to implement real working DR processes that are quick and easy to test, consume little additional storage, and significantly reduce RTO and RPO times.

3.1 VMWARE VCENTER SITE RECOVERY MANAGER

One of the most time-consuming parts of DR failover in a VMware environment is the execution of the steps necessary to connect, register, reconfigure, and power up virtual machines at the DR site.

VMware has solved these problems with the introduction of VMware vCenter Site Recovery Manager. SRM enables two separate VMware environments, the primary and the DR (or paired) sites, to communicate with

each other. Virtual machines can be quickly and easily collected into groups that share common storage resources and can be recovered together.

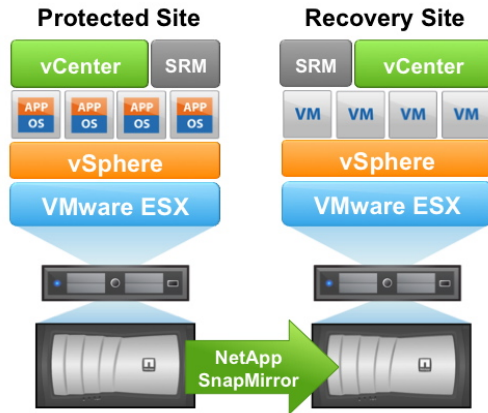


Figure 1 SRM Site Components

Upon the execution of a disaster recovery plan SRM will:

- Quiesce and break the NetApp SnapMirror relationships.
- Connect the replicated datastores to the ESX hosts at the DR site.
- If desired, power off virtual machines, such as test/dev instances, at the DR site, freeing compute resources.
- Reconfigure the virtual machines as defined for the network at the DR site.
- Power on the virtual machines in the order defined in the recovery plan.
- Execute any custom commands that have been stored in the recovery plan

Upon the execution of a disaster recovery test SRM will:

- Create FlexClone volumes of the FlexVol volumes on the DR storage appliance.
- Connect the FlexClone volumes to the ESX hosts at the DR site.
- Connect the virtual machine network adapters to a private test bubble network.
- Reconfigure the virtual machines as defined for the network at the DR site.
- Power on the virtual machines in the order defined in the recovery plan.
- Execute any custom commands that have been stored in the recovery plan

3.2 NETAPP SNAPMIRROR

NetApp SnapMirror™ provides data replication in a SRM and NetApp environment. Built on NetApp Snapshot™ technology, SnapMirror replication is extremely efficient because it only replicates the 4KB blocks that have been changed or added since the previous update. Additional efficiency is gained when SnapMirror is combined with FAS deduplication. When FAS deduplication is utilized on the primary storage, only unique data is replicated to the DR site. Additionally SnapMirror Network Compression can provide native on wire compression of data sent over the WAN. These technologies result in significant telecommunication and storage capacity savings at the DR site. SnapMirror is easily configured using NetApp Protection Manager software, the Data ONTAP® CLI, or FilerView® GUI.

For cases when primary storage is not completely lost, SnapMirror provides an efficient means of resynchronizing the primary and DR sites. SnapMirror can resynchronize the two sites, transferring only changed or new data back to the primary site from the DR site by simply reversing the SnapMirror relationships.

3.3 NETAPP FLEXCLONE

When NetApp FlexClone® technology is combined with SnapMirror and SRM, testing the DR solution can be performed quickly and easily, requiring very little additional storage, and without interrupting the replication process. FlexClone quickly creates a read-writable copy of a FlexVol® volume. When this functionality is used, an additional copy of the data is not required, for example for a 10GB LUN, another 10GB LUN isn't required, only the meta-data required to define the LUN. FlexClone volumes only store data that is written or changed after the clone was created.

The SRM DR testing component leverages FlexClone functionality to create a copy of the DR data in a matter of seconds, requiring only a small percentage of additional capacity for writes that occur during testing.

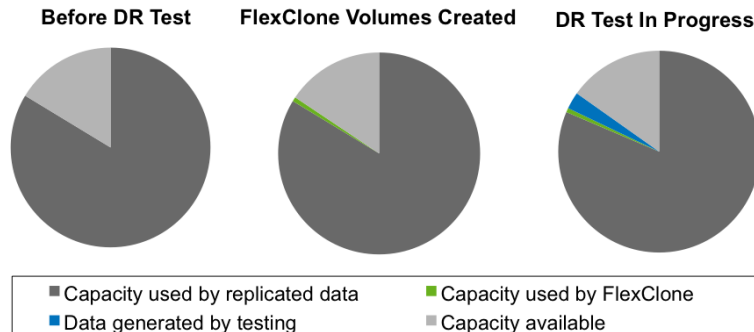


Figure 2 Example capacity required for DR testing with NetApp FlexClone

FlexClone volumes share common data blocks with their parent FlexVol volumes but behave as independent volumes. This allows DR testing to be completed without affecting the existing replication processes. Testing of the DR environment can be performed, even for an extended period of time, while replication is still occurring to the parent FlexVol volume in the background.

3.4 UNIFIED ARCHITECTURE FLEXIBILITY

All NetApp storage systems run the Data ONTAP operating system. This allows for systems with differing performance characteristics and different costs to be utilized at the primary and DR sites. For example, depending on the capabilities required, the DR site might contain a lower model storage system, SATA disk vs. FC disk, or the iSCSI protocol vs. FC. A unified architecture, from the low end of the NetApp storage product line to the high end, also allows for one management and monitoring paradigm to be learned and used by system administrators.

3.5 NEW FEATURES IN SRM FOR VSPHERE

The first version of SRM to support vSphere environments adds support for datastores connected by the NFS protocol. Customers who have taken advantage of the capabilities provided by NetApp and the NFS protocol for VMware environments can now deploy SRM. NetApp has provided a new storage adapter for SRM to support NFS environments.

The new version of SRM also provides a new feature called shared recovery sites. Shared recovery sites allow one vSphere environment to be used to provide DR protection for multiple protected or primary sites. This feature requires multiple SRM servers at the single DR site and a single SRM server at each primary site. Installing an SRM server at each protected site and a corresponding SRM server for each of those in the recovery site, you can enable a single shared DR site to protect multiple remote offices or multiple service provider customers. Please see the VMware documentation for more information regarding setup of SRM servers to support the shared recovery site model.

3.6 NEW FEATURES IN THE NETAPP SRM ADAPTER FOR VSPHERE

NetApp has released a new unified storage adapter for vSphere SRM environments. Starting with version 1.4.3 this unified storage adapter supports new features that were not present in previous releases:

Unified protocol support – The unified storage adapter allows for protection and recovery of virtual machines with data in datastores using different connectivity protocols at the same time. For example with the new unified adapter a virtual machine system disk may be stored in NFS, while iSCSI or FC RDM devices are used for application data.

MultiStore vFiler support – The new adapter supports the use of MultiStore vFilers (virtual storage arrays) configured as arrays in SRM. A vFiler may be added at each site for both the source and destination array with NetApp SnapMirror relationships defined in the destination vFiler.

Non-quieted SMVI snapshot recovery support – The unified adapter supports an option to recover VMware datastores while reverting the NetApp FlexVol volume to the NetApp Snapshot created by SnapManager for Virtual Infrastructure. Please see the appendix for information about non-quieted SMVI snapshot recoverability provided in this release.

The rules for supported replication layouts described in section 5.5 must be followed in multiprotocol environments as well as environments using vFilers.

OBTAINING SITE RECOVERY MANAGER SOFTWARE

VMware vCenter Site Recovery Manager software, as well as the supported storage adapters, can be found at the VMware software download site: www.vmware.com/download/srm.

The individual NetApp storage adapters and documentation can also be downloaded from NOW™ (NetApp on the Web) at <http://NOW.netapp.com>.

4 ENVIRONMENT DESIGNS

This section provides details specific to the storage environment as well as other important design aspects to consider when architecting a solution including SRM.

4.1 ENVIRONMENT DESCRIPTION

The layout of the environment used to document the process of implementing VMware SRM on NetApp storage consisted of the following:

A production site, referred to as Site1 or the primary site, containing:

- Two VMware ESX hosts configured in an HA/DRS cluster
- A NetApp FAS HA system to provide storage for VMFS or NFS datastores
- A physical Windows® 2003 server running VMware vCenter Server and SRM
- A virtual Windows 2003 server, Site1DC, providing Active Directory and DNS services in the primary site
- Various other virtual machines

A disaster recovery site, referred to as Site2 or the DR site, containing:

- Two VMware ESX hosts configured in an HA/DRS cluster
- A NetApp FAS HA system providing storage for VMFS or NFS datastores
- A virtual Windows 2003 server running VMware vCenter Server and SRM
- A virtual Windows 2003 server, providing Active Directory and DNS services in the DR site

NetApp SnapMirror is used to replicate FlexVol volumes containing VMFS datastores from the primary site to the DR site. All virtual machines at the primary site are protected by SnapMirror replication and SRM.

The Windows servers, Site1DC and Site2DC, are domain controllers in the same Active Directory forest. Both servers are configured to be Active Directory Global Catalog servers.

See the image below for a logical description of the layout of the environment.

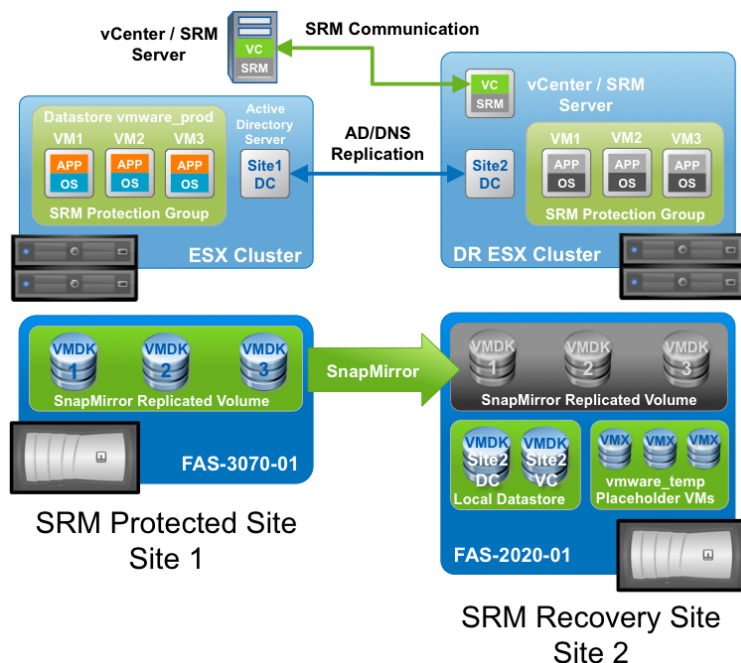


Figure 3 SRM Environment Layout

4.2 IP ADDRESS CHANGES

Some environments may be able to use the same network IP addresses at both the primary site and the DR site. This is referred to as a stretched VLAN or stretched network setup. Other environments may have a requirement to use different network IP addresses (in different VLANs) at the primary site than what is configured at the DR site. SRM supports both of these scenarios.

VMware provides a tool called the dr-ip-customizer to assist with configuring SRM to automatically update VM IP address and network information (such as primary and secondary DNS server settings) when failover occurs (both DR test and real failover). Directions for using the utility are provided in the “SRM Administrator Guide” in the section titled “Customize IP Properties for a Group of Virtual Machines”. The dr-ip-customizer utility is a tool that generates a unique customization specification for each VM, and applies that customization specification to the recovery plan for each VM.

In the design in this document both the primary and DR site are on the same network in a stretched VLAN scenario.

4.3 NFS STORAGE CONNECTIVITY

In NFS environments the storage network used for connecting to NFS datastores is often a private back end network that is either physically or logically separated from the virtual machine network. Networks can be separated on different physical switches, on different physical ports on a shared switch infrastructure using VLANs, or on the same ports by using VLAN tagging.

In some cases multiple private networks may be configured between an ESX host and an individual NetApp controller of vFiler for NFS storage. This practice is sometimes used or recommended to increase overall available throughput between a single ESX host and a single NetApp controller. Some datastores are accessed on one controller IP, and other datastores are accessed on a different IP on that same controller. This does not increase throughput to any one particular datastore, but increases overall throughput between a single ESX host and a single NetApp controller. Configuring multiple networks is only done in environments where certain Etherchannel configurations are not possible. For more information about NFS network design for VMware vSphere on NFS environments, see the networking section of the NetApp and VMware vSphere Storage Best Practices document TR-3749 at <http://media.netapp.com/documents/tr-3749.pdf>.

SRM and the NetApp adapter will support connecting to a datastore over a private storage network rather than the network or ports used for system administration, virtual machine access, user access, and so on. This support is provided by the addition of a new field, called NFS IP Addresses, in the NetApp adapter setup screen in the SRM array manager configuration wizard.

To support private back end NFS storage networks, addresses of the storage controller that are used to serve NFS from that controller to the ESX hosts must be entered in the NFS IP Addresses field. If the controller uses multiple IP addresses to serve NFS data, these IP addresses are entered in the NFS IP Addresses field and are separated by commas.

If specific IP addresses are not entered in the NFS IP Addresses field to use for NFS datastore connections, then the disaster recovery NAS adapter returns all available IP address of the storage controller to SRM. When SRM performs a DR test or failover, it will attempt to make NFS mounts to every IP address on the controller, even ones that the ESX hosts would be unable to access from the VMkernel ports such as addresses on other networks.

Below is a simple diagram showing the IP addresses used in the DR site of the NAS environment. In a later section of this document we will see the NFS IP addresses shown here entered into the NAS adapter in the SRM array configuration wizard.

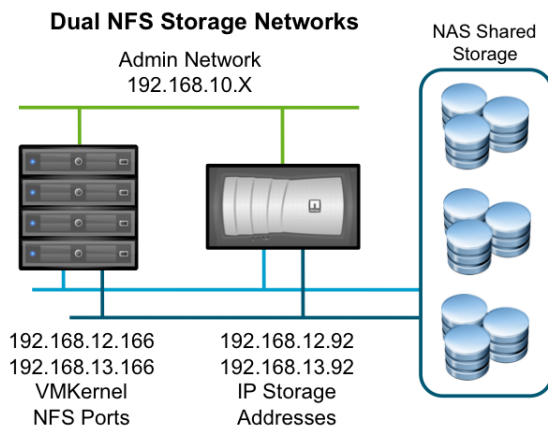


Figure 4 Dual NFS Storage Networks Example

4.4 DR TESTING NETWORK CONSIDERATIONS

When a DR test is performed, a private test bubble network is created on the ESX host for the virtual machines, however this network is not automatically connected to any physical network adapters and so provides no connectivity between ESX hosts. To allow communication among virtual machines running on different ESX hosts during DR testing, a physical private network has been created between the ESX hosts at the DR site. To accomplish this, the test bubble network can be separated physically or by using VLANs or VLAN tagging. Segregating this network from the production network is required.

4.5 ACTIVE DIRECTORY SERVICES CONSIDERATIONS

The Active Directory/DNS architecture plays an important role in successful failover, DR test, and failback scenarios. AD servers should not be recovered from replicas created by unsupported processes because this could create a USN rollback scenario. See [MS KB888794](http://support.microsoft.com/kb/888794/) <http://support.microsoft.com/kb/888794/> for information regarding supported methods of creating backups of AD servers in virtual server environments.

PROVIDING ACTIVE DIRECTORY SERVICES FOR SRM DR TESTING

To provide name resolution and user authentication services in the private DR test network an AD server at the DR site may be cloned prior to running the DR test. Before powering on the VM reconfigure the VMs network connections to connect the cloned AD server only to the DR test network. The AD server chosen to clone must be one that was configured as a global catalog server. Some applications and AD functions require FSMO roles in the Active Directory forest. To seize the roles on the cloned AD server in the private test network use the procedure described in Microsoft KB: <http://support.microsoft.com/kb/255504>. After the

roles are seized it is very important that the clone never be connected to a production VM Network, and that it is destroyed after DR testing is complete.

PROVIDING ACTIVE DIRECTORY SERVICES FOR SRM FAILOVER

For a real DR failover scenario, the AD cloning process is not required. In the SRM failover scenario, the existing AD and name resolution servers at the recovery site provide those services. However, the five FSMO roles must be seized per the procedure described in the Microsoft KB at <http://support.microsoft.com/kb/255504>

5 REQUIREMENTS

5.1 SUPPORTED STORAGE PROTOCOLS

SRM 1.0.X provides support for VMFS datastores and RDM devices (FC or iSCSI) only.

The vSphere version of SRM (4.0) provides support for VMFS datastores, RDM devices, and NFS datastores.

The unified SRM adapter allows a virtual machine to have data in an NFS datastore as well as a iSCSI or FC datastores or RDM devices. A virtual machine system disk may be stored in NFS, while iSCSI or FC RDM devices in the same VM are used for application data.

5.2 SRM/SRA VERSION DEPENDENCIES

Specific versions of the NetApp SRA are required to support different versions of VMware SRM. Please see the table below regarding which versions of SRM and the NetApp SRA are supported together.

NetApp SRA Version	VMware vCenter SRM Version		
	V1.0	V1.0U1	V4.X*
v1.0 SAN	Yes	No	No
v1.0.X SAN	No	Yes	No
v1.4 to 1.4.2 SAN or NAS*	No	No	Yes
v1.4.3 (unified)**	No	No	Yes
v1.4.3P1 (unified)**	No	No	Yes

Table 1 NetApp SRA and VMware SRM compatibility

* NFS support with SRM requires vCenter 4.0 and is supported with ESX 3.0.3, ESX/ESXi 3.5U3+, and ESX/ESXi 4.0. SRM 4.0 is not supported with Virtual Center 2.5.

** Combining NAS and SAN storage protocols for the same VM requires version 1.4.3.

5.3 SRA AND DATA ONTAP VERSION DEPENDENCIES

Certain versions of the SRA require specific versions of the Data ONTAP operating system for compatibility. Please see the table below regarding which versions of Data ONTAP and the NetApp SRA are supported together.

NetApp SRA Version	NetApp Data ONTAP version required
v1.0 SAN	7.2.2+
v1.0.X SAN	7.2.2+
v1.4 to v1.4.2 SAN	7.2.2+
v1.4 to v1.4.2 NAS	7.2.4+
V1.4.3	7.2.4+
v1.4.3 (using vFiler support)	7.3.2+

Table 2 NetApp SRA and Data ONTAP version compatibility

5.4 SUPPORTED REPLICATION TECHNOLOGIES

The NetApp SRA supports the following data replication technologies:

- Asynchronous volume SnapMirror
- Asynchronous qtrees SnapMirror
- Synchronous SnapMirror

The NetApp SRA does not support the following replication technologies:

- SnapVault®
- SyncMirror® replication between SRM sites (as in MetroCluster)
Note: A MetroCluster system may serve as the source or destination of SnapMirror relationships in an SRM environment. However, SRM does not manage MetroCluster failover or the failover of SyncMirror relationships in MetroCluster.

5.5 SUPPORTED REPLICATION LAYOUTS

Each storage controller or vFiler in a NetApp FAS system is considered an array in SRM. SRM supports certain array-to-array (or controller-to-controller) replication layouts. To determine supportability, keep this rule in mind: A single virtual machine cannot own data (vmdk or RDM) on more than one array or vFiler.

Relationships where the data (vmdk or RDM) owned by any individual virtual machine exists on only one array (physical controller or vFiler) at each site are supported. The SnapMirror relationship layout scenarios shown here are supported. Each virtual machine in the replicated volumes owns data on only one array within each site.

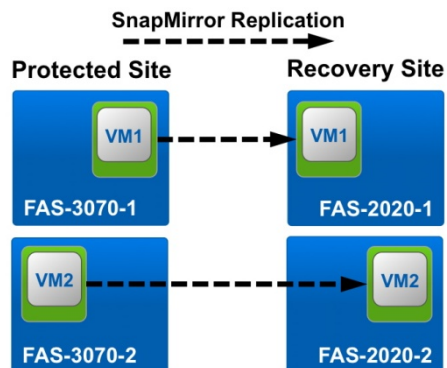


Figure 5 Supported Replication Example

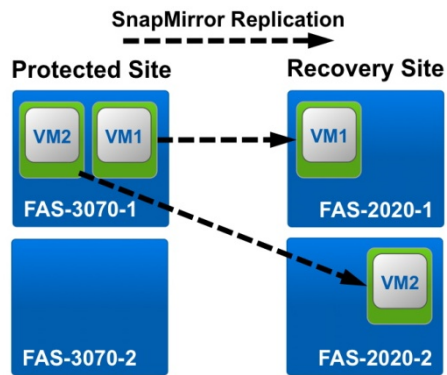


Figure 6 Supported Replication Example

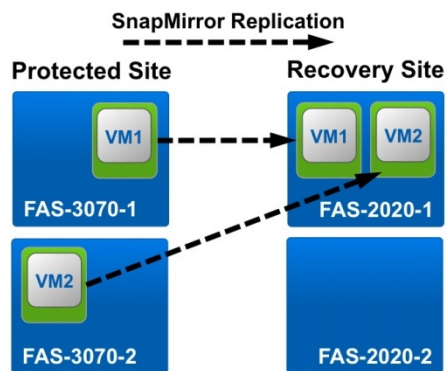


Figure 7 Supported Replication Example

Relationships where the data (vmdk or RDM) owned by any individual virtual machine exists on multiple arrays (physical controller or vFile) are not supported. In the examples below VM5 cannot be configured for protection with SRM because VM5 has data on two arrays.

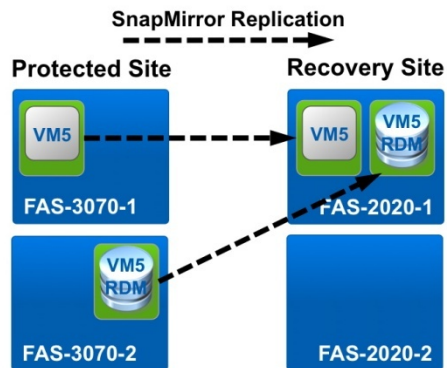


Figure 8 Unsupported Replication Example

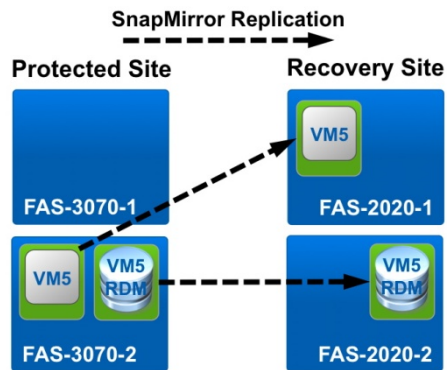


Figure 9 Unsupported Replication Example

Any replication relationship where an individual NetApp volume or qtree is replicated from one source array to multiple destination arrays is not supported by SRM. In this example VM1 cannot be configured for protection in SRM because it is replicated to two different locations.

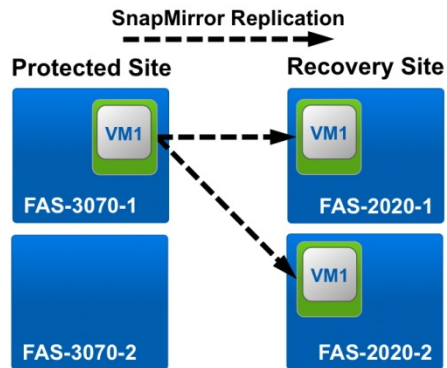


Figure 10 Unsupported Replication Example

5.6 MULTISTORE VFILER REQUIREMENTS

MultiStore enables secure logical partitioning of a single NetApp storage controller into virtual controllers called vFilers. vFilers have the effect of making a single physical storage controller appear to be many logical controllers. Each vFiler can be individually managed with different sets of performance and policy characteristics. vFilers support IP storage environments including iSCSI VMFS datastores, iSCSI RDM devices, and NFS datastores.

The following are requirements for MultiStore vFiler support with the NetApp SRA:

- The source and destination vFiler must both be online.
- SnapMirror relationships must be defined within the vFiler context, not on the physical hosting array referred to as vFiler0.
- Each vFiler at the primary site must be added to SRM separately as an array.
- Each vFiler at the DR site must be added to SRM separately as an array.
- Prior to executing a DR test the option `vfiler.vol_clone_zapi_allow` must be set to on on the physical controller.
- Only iSCSI or NFS connected datastores are supported in vFilers.

- In iSCSI environments ESX hosts at the DR site must have established iSCSI sessions to the DR site vFiler prior to executing SRM DR test or failover. The NetApp adapter does not start the iSCSI service in the vFiler or establish an iSCSI connection to the iSCSI target.
- In iSCSI environments the DR site vFiler must have an igroup of type "vmware" prior to executing SRM DR test or failover. The NetApp adapter does not create the "vmware" type igroup in the DR site vFiler.
- In a NFS environment VMkernel port network connectivity to the DR vFiler NFS IP addresses must already exist prior to executing SRM DR test or failover. Ensure that network communication is possible between the VMkernel ports on the ESX hosts and the network interfaces on the NetApp controller, which provide NFS access. For example, ensure appropriate VLANs have been configured if using VLAN tagging.
- A single VM must not have data on multiple vFilers. The storage layout rules described in section 4 apply equally to both physical NetApp SRM arrays and vFiler SRM arrays.

5.7 GENERAL ENVIRONMENT REQUIREMENTS

1. vCenter installed at primary and DR sites. VMware SRM requires two independent ESX environments, each managed by its own vCenter server.
2. vSphere client available at primary and DR sites.
3. Site Recovery Manager installed at primary and DR sites.
4. NetApp site recovery adapter installed on the SRM servers at the primary and DR sites.
Note: See the preceding table regarding version dependencies between SRM and the SRA.
5. NetApp FlexVol volumes and FlexClone.
6. LUNs or NFS exports configured as datastores and connected at the primary site.
7. A small LUN or NFS export configured as a datastore at the DR site for storage for placeholder virtual machines.
8. For FC or iSCSI implementations NetApp igroups must pre-exist on the recovery array (physical array or vFiler) and contain the necessary ESX host initiator names. SRM will automatically map LUNs to igroups during failover or DR testing, but igroups are not automatically created. The igroups at the DR site may contain local LUNs for locally running VMs, but LUNs replicated from the primary site should not be preadded to the igroups at the DR site, SRM adds these LUNs automatically during DR test or failover.
9. For NAS implementations the following configuration rules must be followed:
 - a. Exports must be in the /etc/exports file. Manual exports made with the CLI without the -p option will not be discovered by SRM.
 - b. Exports must use values in the RW (read/write) security field in the /etc/exports file. Exports using the default setting of rw to all hosts will not be discovered by SRM.

Example of a /etc/export line that would be discovered by SRM:
/vol/srm5 -rw=192.168.2.0/24,root=192.168.2.0/24

Example of a /etc/export line that would not be discovered by SRM:
/vol/srm5 -rw,anon=0
10. Datastores must contain virtual machines, or virtual disks owned by virtual machines, in the vCenter inventory to be discovered by SRM.
11. The environment used in this technical report was deployed using the best practices documented in TR-3428: NetApp and VMware Virtual Infrastructure 3 Storage Best Practices: www.netapp.com/us/library/technical-reports/tr-3428.html or TR-3749: NetApp and VMware vSphere Storage Best Practices: www.netapp.com/us/library/technical-reports/tr-3749.html.
12. SnapMirror must be configured and replicating the volumes containing datastores to be protected. SRM does not perform SnapMirror updates or baseline transfers. SnapMirror transfers must be managed and

scheduled using NetApp software such as the built-in scheduler in Data ONTAP or Protection Manager software.

6 INSTALLATION AND CONFIGURATION

6.1 OVERVIEW

Configuring SRM to protect virtual machines replicated by SnapMirror involves these steps, summarized here but explained in detail below.

1. Install and enable the SRM plug-in on each of the vCenter servers.
2. Install the NetApp SRA on each of the vCenter servers. The NetApp adapter must be installed on each SRM server prior to configuring arrays in SRM.
3. Pair the SRM sites. This enables the SRM communication between the sites.
4. Configure storage array managers. This enables the SRM software to communicate with the NetApp storage appliances for issuing SnapMirror quiesce/break commands, mapping LUNs to igroups, and so on.
5. Build SRM protection groups at the primary site. Protection groups define groups of virtual machines that will be recovered together and the resources they will utilize at the DR site.
6. Build SRM recovery plans at the DR site. Recovery plans identify the startup priority of virtual machines, timeout settings for waiting for recovered virtual machines to respond, additional custom commands to execute, and so on.
7. Testing the recovery plan.

6.2 PAIRING PRIMARY AND DR SITES

Each site must have a separate vCenter server with SRM installed and enabled. After installing SRM and enabling it, each vCenter server SRM plug-in indicates there is no paired site, and none of the disaster recovery setup options have been configured.

1. Pair the sites together beginning on the vCenter server at the primary site. Basic SRM configuration is done by working through the options in the Setup section of the main site Recovery Summary tab. To begin pairing the sites, click the Configure link next to the Connection label and enter the address of the DR site vCenter server.
2. Enter the DR site vCenter username and password.
3. At the end of the configuration dialogs, verify that the connection was made successfully.
4. After the site pairing is complete, the primary site vCenter server will display the paired site addresses and “Connected” in the Setup box. Note that the SRM plug-in at the DR site will also display the sites paired in the opposite direction.

Site Recovery for 192.168.10.100

Summary Alarms Permissions

Local Site	Paired Site
VC Server: 192.168.10.100:443	VC Server: 192.168.10.101:443
DR Server: 192.168.10.100:8095	DR Server: 192.168.10.101:8095
Site Name: Site Recovery for 192.168.10.100	Site Name: Site Recovery for 192.168.10.101

Setup

This server has not completed set up for disaster recovery. To complete configuration, follow the steps below.

Connection:	Connected	Configure Break
Array Managers:	Not Configured	Configure
Inventory Preferences:	Not Configured	Configure
Protection Groups:	0 Group(s) Created	Create
Recovery Plans:	0 Plan(s) Created	Create

6.3 USING HTTPS/SSL TO CONNECT TO THE NETAPP CONTROLLERS

By default the NetApp storage adapter connects to the storage array via API using HTTP. The NetApp storage adapter can be configured to use SSL (HTTPS) for communication with the storage arrays. This requires that SSL modules be added to the instance of Perl that is shipped and installed with SRM. VMware and NetApp do not distribute these modules. For the procedure to install the SSL modules and enable SSL communication between the storage adapter and array, please see NetApp KB article [1012531](https://kb.netapp.com/support/index?page=content&id=1012531) <https://kb.netapp.com/support/index?page=content&id=1012531>.

6.4 CONFIGURING ACCESS TO THE NETAPP CONTROLLERS

1. Starting again at the vCenter server in the primary site, click the Configure link next to Array Managers: the Configure Array Managers dialog appears. Click the Add... button to add an array. Remember that NetApp HA systems have two controllers, and each controller must be added as an array in SRM.
Note: Before configuring the array managers, it is recommended that the SnapMirror relationships exist and have replicated datastores for the tool to discover. Without existing SnapMirror relationships, the process of configuring array managers might slightly differ from what is shown here.

2. In the Add Array Manager dialog, select the manager type of "NetApp Data ONTAP Storage System."

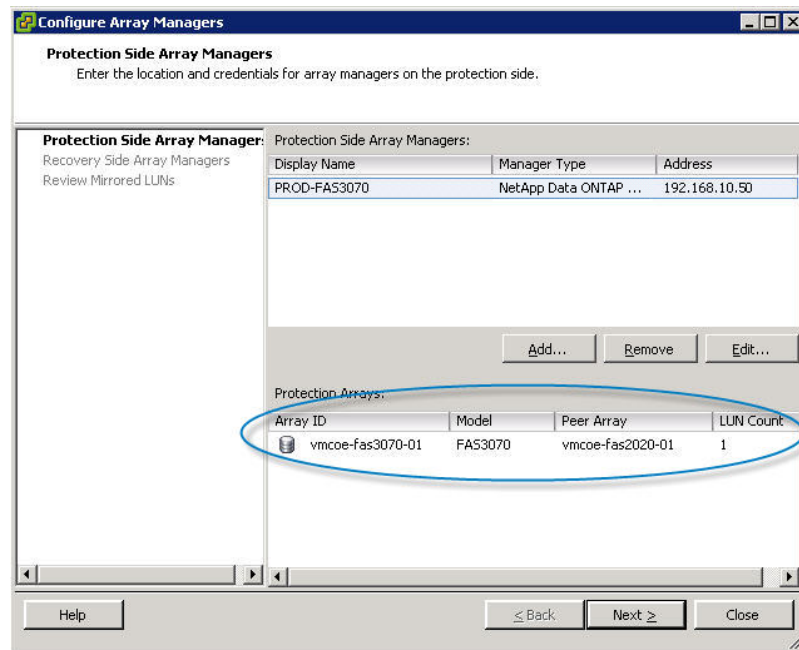
Note: If using either of the protocol specific adapters (version 1.4 through 1.4.2 SAN or NAS) you must select the appropriate array manager type from the manager type drop down and each array must be added separately for each protocol type. If using adapter version 1.4.3 each array need only be added once and the manager type of "NetApp Data ONTAP Storage System" Selected.

Enter a display name and the other information for the primary NetApp storage at Site1. Click the Connect button and verify the controller is discovered. If you have additional NetApp controllers at the primary site, perform this step for each controller. If you are adding MultiStore vFilers, each vFiler must be added separately as an array.

The NFS IP Addresses field is where the IP addresses on the NetApp controller, used to serve NFS to the ESX hosts, are entered with a comma separating each address. This is the protection site array, so these addresses would not actually be used by SRM unless virtual machines were being recovered at this site, however it is a good practice to add them as they could be used later in a failback scenario.

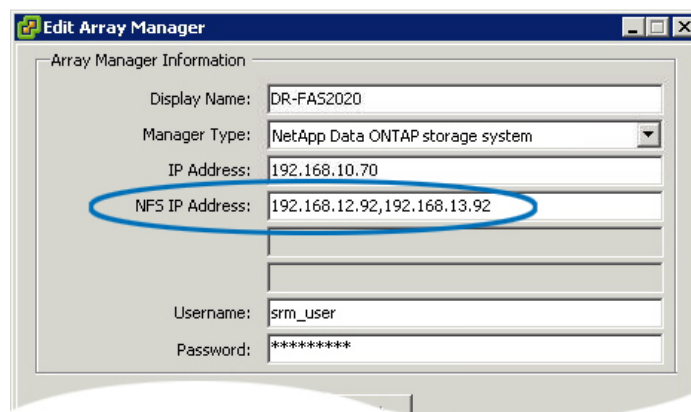
Array ID	Model
☒ vmcoe-fas3070-01	FAS3070

- The protection-side array will be listed at the bottom of the Configure Array Managers window, along with the discovered peer array. The destination of any SnapMirror relationships is listed here, including a count of replicated LUNs discovered by SRM.

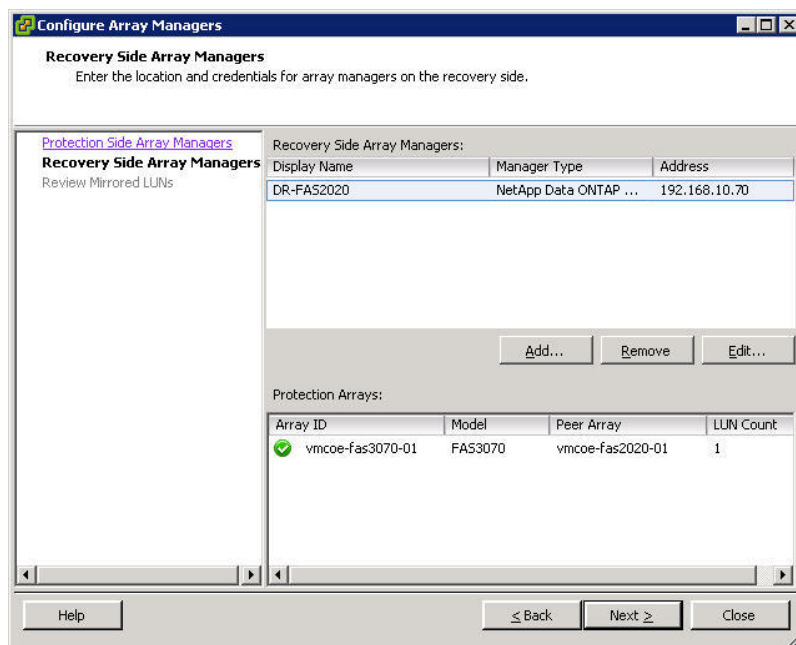


- Click Next and configure recovery-side array managers in the same fashion. Click the Add... button and enter the information for the NetApp controller at the DR site. If you have additional NetApp controllers at the DR site, add these controllers here as well. If you are adding MultiStore vFilers, each vFiler must be added separately as an array.

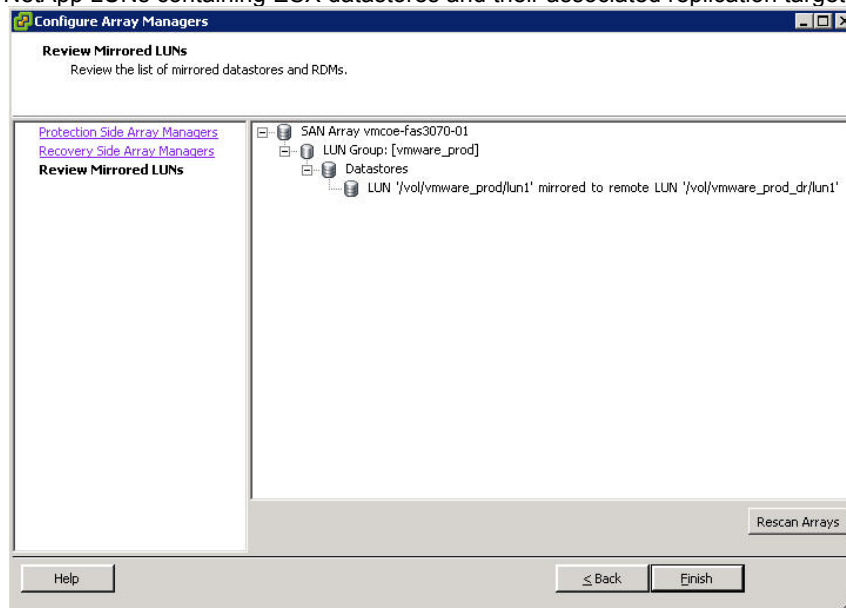
IP addresses on the recovery site NetApp array, which are used to serve NFS to the ESX hosts at the DR site, are entered with a comma separating each address in the NFS IP Addresses field. This is the recovery site array, so SRM will mount NFS datastores on these addresses for DR test and failover.



Once the array is added successfully, the Protection Arrays section at the bottom of the screen will indicate the replicated storage is properly detected.



- After finishing the configuration dialogs, the Review Mirrored LUNs page will indicate all the discovered NetApp LUNs containing ESX datastores and their associated replication targets. Click Finish.



- The array managers must also be configured at the DR site. The adapters are added to array managers in the same manner as above, however the arrays should be added in reverse order. In this SRM server the array at the DR site is considered the protected array, and the array at the primary site is considered the recovery array. In this case there might be no storage being replicated from this site to the other site. So the final screen of the configure array managers wizard might show an error or warning indication that no replicated storage was found. This is normal for a one-way SRM configuration.

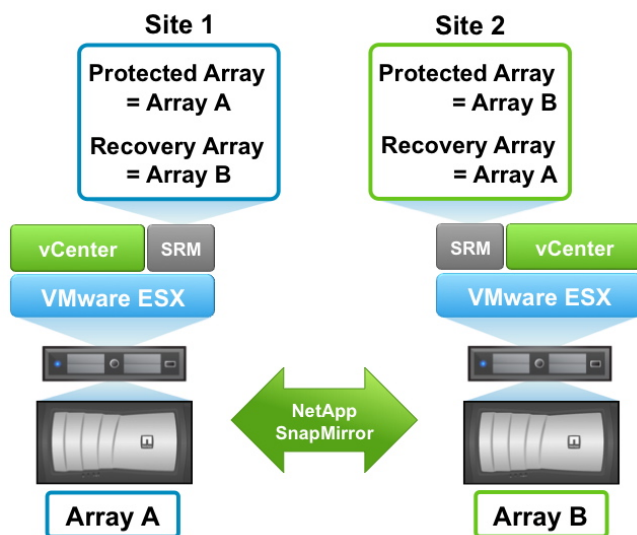
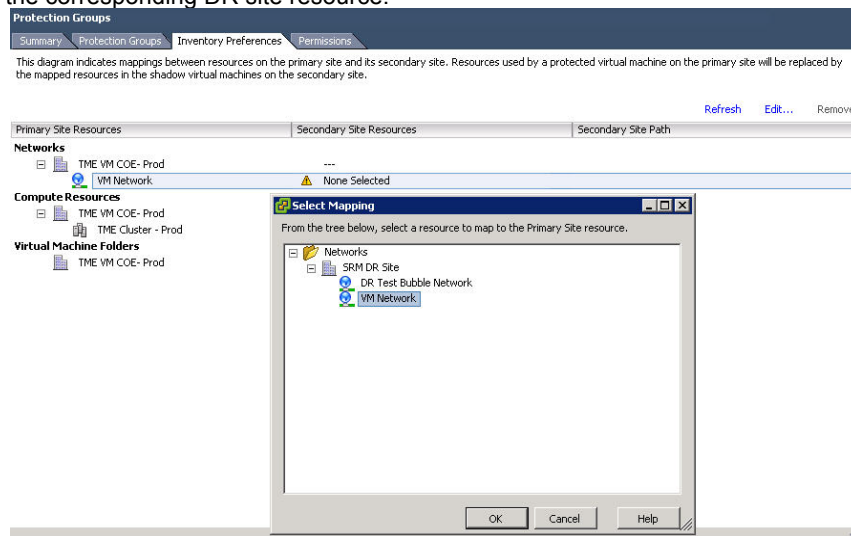


Figure 11 SRM Site and Array Manager Relationships

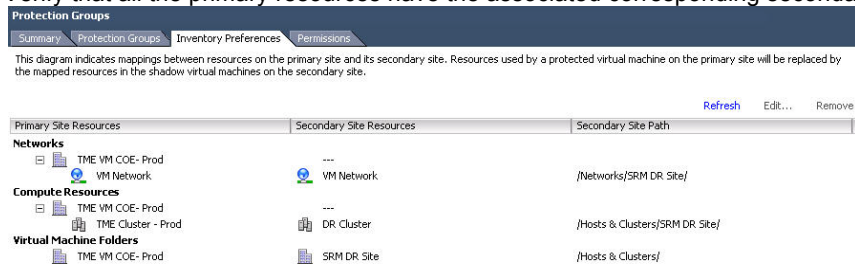
6.5 CONFIGURING INVENTORY PREFERENCES

The VMware environments at the primary site and the DR site might have different sets of resources, such as virtual machine networks, ESX hosts, folders, and so on. In this stage of the configuration, identify a DR site resource for each corresponding resource at the primary site.

1. On the primary site vCenter server, click the Configure link next to Inventory Preferences.
2. For each resource in the Primary Site column, click the resource, and then click the Edit... link. Select the corresponding DR site resource.



3. Verify that all the primary resources have the associated corresponding secondary resources.

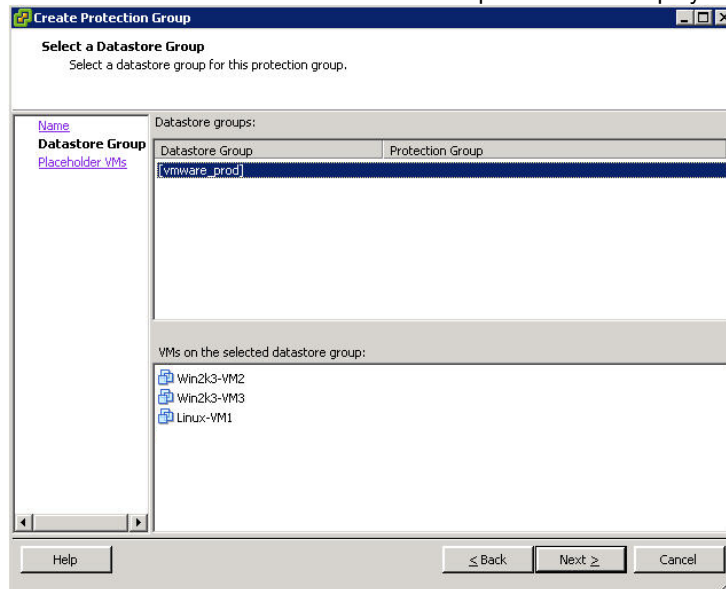


4. Each of the connection, array managers, and inventory preferences steps in the Setup section of the Summary tab should now indicate Connected or Configured.
5. Proceed with building a protection group.

6.6 BUILDING A PROTECTION GROUP

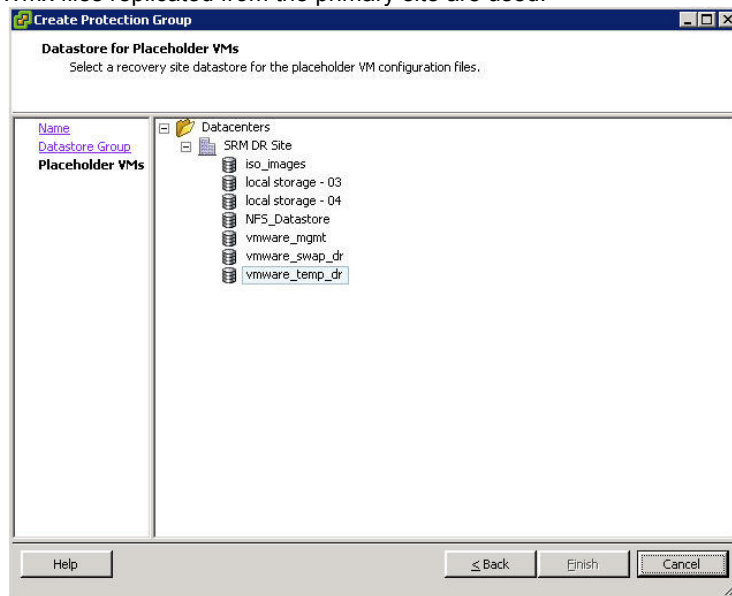
Protection groups allow virtual machines to be collected in groups that will be recovered together. Protection groups are created on the primary site vCenter server and identify which datastores and virtual machines are protected and will be recovered with SRM. In a NetApp environment, using volume SnapMirror (VSM), replication occurs at the FlexVol level. Therefore, SRM protection groups may be easily built using FlexVol volumes as the basis of grouping virtual machines.

1. At the primary site vCenter server, click the Create link next to Protection Groups: Enter a name for the protection group and click Next.
2. Select the datastores to be protected by this group. In this case, the SnapMirror datastore vmware_prod is selected. The virtual machines that will be protected are displayed at the bottom in the window.

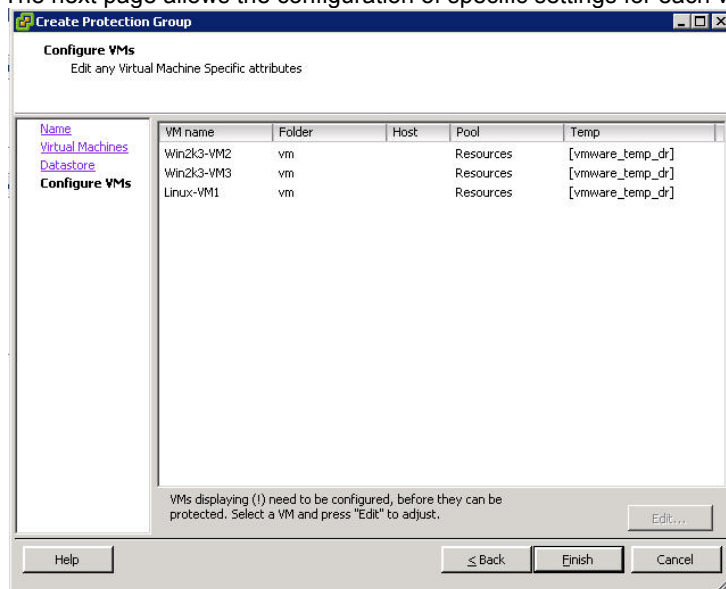


3. SRM creates placeholder virtual machines in the environment at the DR site. In the next step, select a datastore that will contain the placeholder virtual machines. In this case, a datastore called vmware_temp_dr has already been created at the DR site for the purpose of storing the placeholder virtual machines. This datastore need only be large enough to contain a placeholder .vmx file for each virtual machine that will be part of a protection group. During DR tests and real DR failovers the actual

.vmx files replicated from the primary site are used.

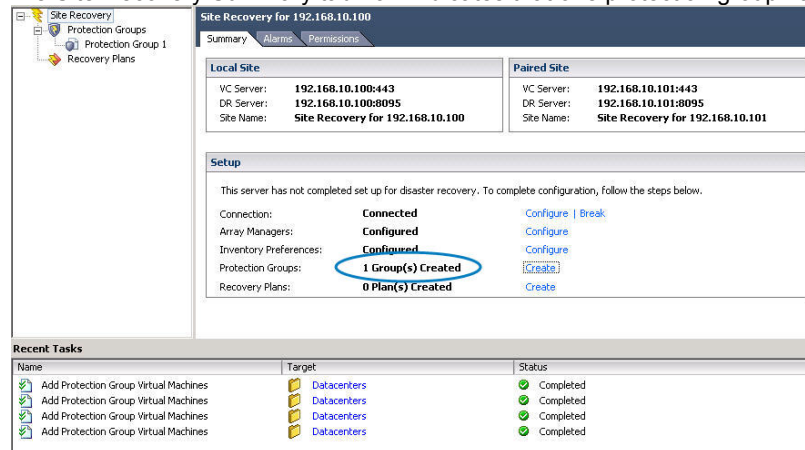


4. The next page allows the configuration of specific settings for each virtual machine.

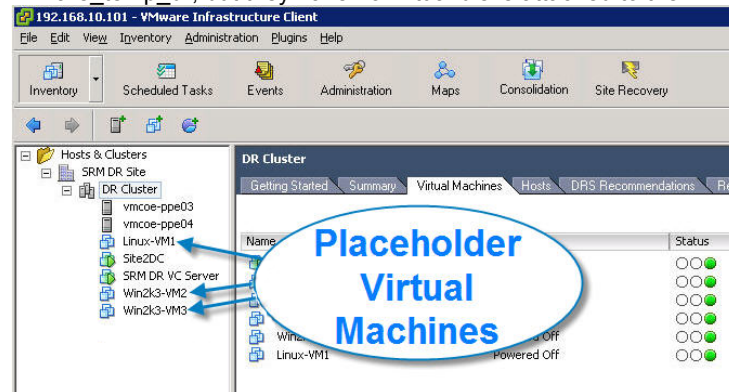


Note: In this example, as we have not separated the transient data in this environment, we finish the wizard here. If the Windows virtual machines have been configured to store virtual memory pagefiles in vmdks on nonreplicated datastores, see the appendix describing the configuration necessary to support this and how to set up SRM to recover those virtual machines.

- The Site Recovery Summary tab now indicates that one protection group has been created.



Note that in vCenter at the DR site a placeholder virtual machine has been created for each virtual machine that was in the protection group. These virtual machines have .vmx configuration files stored in vmware_temp_dr, but they have no virtual disks attached to them.



6.7 CREATING A RECOVERY PLAN

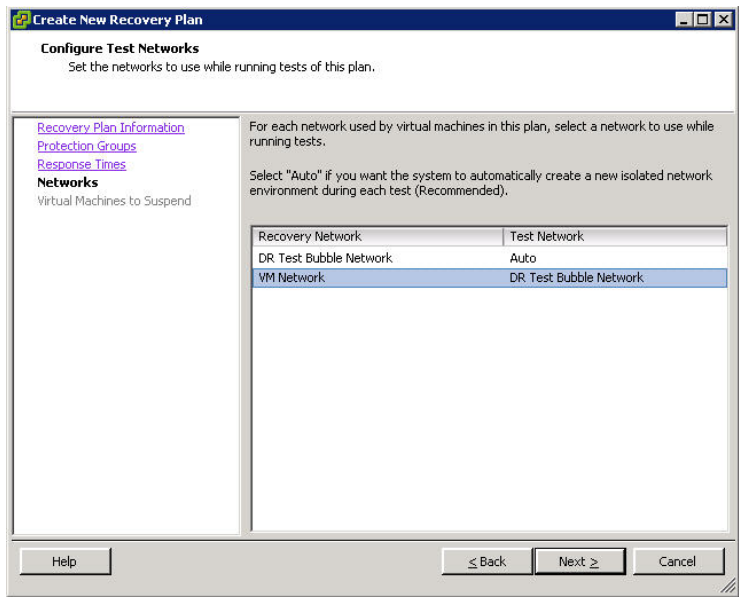
Recovery plans are created in the vCenter server at the DR site. Each recovery plan contains one or more of the protection groups created at the primary site. All of the protection groups contained in a recovery plan will be recovered by SRM when that plan is executed.

- In the vCenter server at the DR site click the Create link next to Recovery Plans. Enter a name for this recovery plan and click Next.

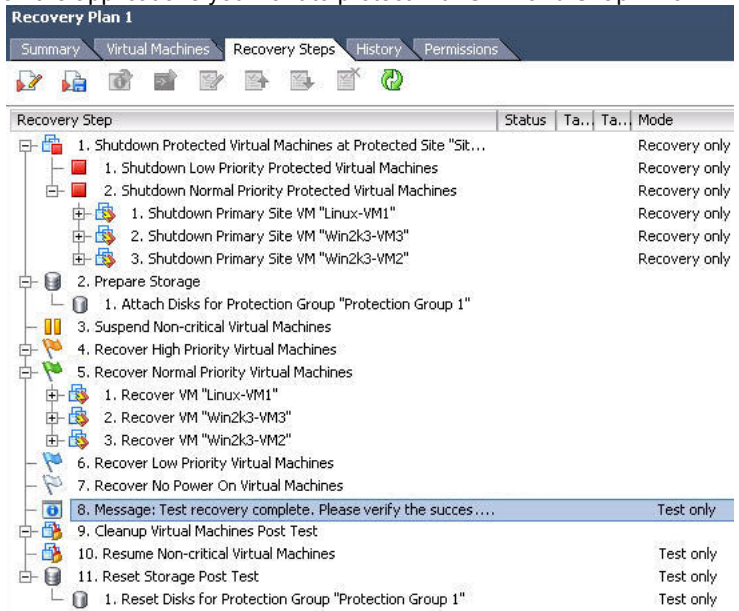


- The protection group created at the primary site will be shown in the dialog box. Select the group and click Next.
- If necessary, adjust the virtual machine response times. These are the times allotted that SRM will wait for a response from VMware tools in the guest to indicate that the virtual machine has completed power on. It's generally not necessary to adjust these values.
- Configure a test network to use when running tests of this recovery plan. If the test network for a recovery network is set to Auto, then SRM will automatically create a "test bubble" network to connect to the virtual machines during a DR test. However, if a "DR test bubble network" already exists in this

environment as described in the design section, then that network is selected as the test network for the virtual machine network. No test network is necessary for the DR test bubble network itself, so it remains set to Auto.



- 5. Next select virtual machines to suspend. SRM allows virtual machines that normally run local at the DR site to be suspended when a recovery plan is executed. An example of using this feature might be suspending development/test machines to free up compute resources at the DR site when a failover is triggered.
- 6. Click Finish to close the dialog, and then review the Recovery Plan 1 Summary tab. The Status indicates the protection group is “OK.”
- 7. Review the recovery plan just created. Note that SRM creates a Message step, which will pause the recovery plan while DR tests are performed. It is during this pause that testing of the DR environment functionality is performed within the DR test bubble network. The tests that would be performed depend on the applications you want to protect with SRM and SnapMirror.



7 EXECUTING RECOVERY PLAN: TEST MODE

When running a test of the recovery plan SRM creates a NetApp FlexClone of the replicated FlexVol Volume at the DR site. The datastore in this volume is then mounted to the DR ESX cluster and the virtual machines configured and powered on. During a test, the virtual machines are connected to the DR test bubble network rather than the public virtual machine network.

The following figure shows the vSphere client map of the network at the DR site before the DR test. Note the virtual machines that are not running are the placeholder virtual machines created when the protection group was set up.

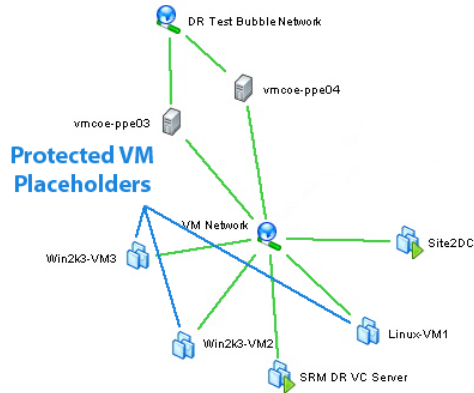


Figure 12 Screenshot of VM to Network Map View in vCenter Client

The ESX host used to start each VM in the recovery plan is the host on which the placeholder VM is currently registered. To help make sure that multiple VMs can be started simultaneously you should evenly distribute the placeholder VMs across ESX hosts before running the recovery plan. Make sure to do this for the VMs in each step of the recovery plan. For example ensure that all the VMs in the high priority step are evenly distributed across ESX hosts, then make sure all the VMs in the normal priority step are evenly distributed, and so on. If running VMware DRS the VMs will be distributed across ESX hosts during startup and it is not necessary to manually distribute the placeholder VMs. SRM will startup two VMs per ESX host, up to a maximum of 18 at a time, while executing the recovery plan. For more information about SRM VM startup performance see VMware vCenter Site Recovery Manager 4.0 Performance and Best Practices for Performance at www.vmware.com/files/pdf/VMware-vCenter-SRM-WP-EN.pdf

1. To provide Active Directory and name resolution services in the DR test network, clone an AD server at the recovery site prior to running the DR test. Before powering on the clone, make sure to reconfigure the network settings of the cloned AD server to connect it only to the DR test network. The AD server chosen to clone must be one that was configured as a global catalog server. Some applications and AD functions require FSMO roles in the Active Directory forest. To seize the roles on the cloned AD server in the private test network use the procedure described in Microsoft KB: <http://support.microsoft.com/kb/255504>. The five roles are Schema master, Domain naming master, RID master, PDC emulator, Infrastructure master. After the roles are seized it is very important to ensure that the clone never be connected to a production VM Network, and that it is destroyed after DR testing is complete.
2. Prepare to run the test by connecting to the vCenter server at the DR site. Select the recovery plan to test on the left and open the Recovery Steps tab on the right.
3. Verify that the SnapMirror relationships have been updated so that the version of data you want to test has been replicated to the DR site.
4. Click Test to launch a test of the recovery plan. If you are still connected to the NetApp console you will see messages as the NetApp adapter creates FlexClone volumes and maps the LUNs to the igroups or

creates NFS exports. Then SRM initiates a storage rescan on each of the ESX hosts.

Configuration Tasks & Events Alarms Permissions Maps					
Storage Refresh Remove Add Storage...					
Identification	Device	Capacity	Free	Type	
snap-608b0d2d-vmware_prod	vmhba32:1:0:1	49.75 GB	5.71 GB	vmfs3	
iso_images	192.168.10.50:/vol/iso_im...	40.00 GB	27.65 GB	NFS	
vmware_mgmt	vmhba32:1:20:1	49.75 GB	38.74 GB	vmfs3	
vmware_swap_dr	vmhba32:1:10:1	49.75 GB	47.24 GB	vmfs3	
vmware_temp_dr	vmhba32:1:17:1	49.75 GB	49.24 GB	vmfs3	
local storage - 03	vmhba0:0:0:5	59.50 GB	58.89 GB	vmfs3	
NFS Datastore	192.168.10.50:/vol/nfs_da...	400.00 GB	265.92 GB	NFS	

If you are using NFS storage the adapter will create NFS exports, exporting the volumes to each VMkernel port reported by SRM and SRM will mount each exported volume.

Below is an example of NFS datastores being mounted by SRM at the DR site during a DR test. Note that SRM uses each IP address that was provided in the NFS IP Addresses field above. The first recovered datastore is mounted at the first NFS IP address provided. All ESX hosts mounting that datastore use this same IP. Then the second datastore being recovered is mounted at the second NFS IP address, likewise by all ESX hosts accessing the datastore. This is required to make sure that all ESX hosts recognize the same mounts as the same datastores.

Datastores Refresh Delete Add Storage...						
Identification	Status	Device	Capacity	Free	Type	
srm1	✓ Normal	192.168.12.92:/vol/testfailoverC...	60.00 GB	54.01 GB	NF	
srm2	✓ Normal	192.168.13.92:/vol/testfailoverC...	60.00 GB	54.05 GB	NF	
srm3	✓ Normal	192.168.12.92:/vol/testfailoverC...	15.00 GB	13.50 GB	NF	
srm4	✓ Normal	192.168.13.92:/vol/testfailoverC...	15.00 GB	13.50 GB	NF	
srm5	✓ Normal	192.168.12.92:/vol/testfailoverC...	15.00 GB	13.50 GB	NF	
srm5a	✓ Normal	192.168.13.92:/vol/testfailoverC...	5.00 GB	4.99 GB	NF	
srm6	✓ Normal	192.168.13.92:/vol/testfailoverC...	15.00 GB	13.50 GB	NF	
srm6a	✓ Normal	192.168.12.92:/vol/testfailoverC...	5.00 GB	4.99 GB	NF	
Storage1	✓ Normal	Local ATA Disk (t10.ATA____...	300.25 GB	292.08 GB	vm	

SRM continues mounting datastores on all ESX hosts (which ESX hosts is determined by SRM inventory mappings), alternating between each NFS IP address provided as each datastore is recovered. SRM does not currently provide a mechanism to specify which IP address should be used for each datastore. Some environments might have two, three, four, or more IP addresses on the NetApp array to enter into the NFS IP Addresses field.

- After all the virtual machines have been recovered and the test run of the recovery plan has paused, the network map in the vSphere client will change as shown here that recovered virtual machines have been connected to the bubble network. A test of the functionality of the virtual machines in the bubble network can now be performed.

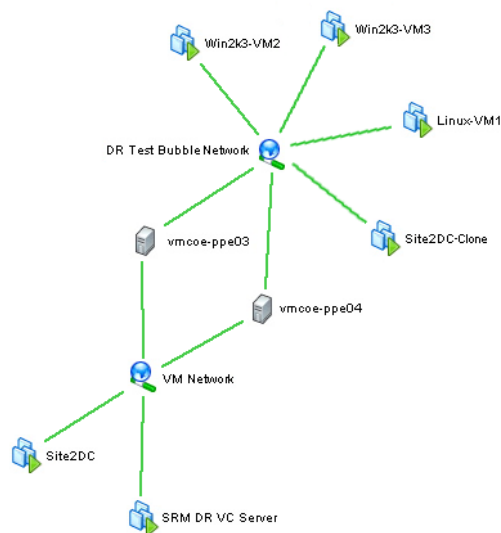


Figure 13 Screenshot of VM to Network Map view in vCenter Client while in DR Test Mode

6. When completed with DR testing, click the continue link in the Recovery Steps tab. SRM will bring down the DR test environment, disconnect the LUN, clean up the FlexClone volume, and return the environment to normal.
7. If you cloned an Active Directory/DNS server at the DR site it can now be shut down, removed from inventory, and deleted. A new clone should be created if re-running DR tests after some time, as the windows security information in the AD server may become outdated if not updated periodically. Again, ensure that the cloned AD server is never connected to a public VM Network.

8 EXECUTING RECOVERY PLAN: TRUE DR SCENARIO

8.1 REQUIREMENTS AND ASSUMPTIONS

Every environment has its own unique characteristics; each environment can have an effect on a DR plan. Depending on the type of DR solutions deployed, each organization's DR situation could be very different. To make sure of success, you require proper planning, documentation, and a realistic walkthrough of a DR scenario.

To provide a successful DR experience, consider some general requirements and assumptions. This is not an all-inclusive list. There are many variables to plan for depending on the configuration of each environment.

- The SRM on NetApp environment has been set up properly, and all SRM recovery plans have been tested successfully.
- During recovery plan testing, the functionality of the environment was verified.
- Systems administrators have access to a workstation or server desktop session from which to administer the DR site and perform the failover.
- Systems administrators have all appropriate credentials, accounts, passwords, and so on required to access the systems.
- Connectivity to the DR network is available from where every operations will be performed.
- Certain infrastructure servers already exist in the DR site and are accessible. These systems provide basic services necessary for the administrators to work in the environment and execute the recovery plan.
 - The DR site vCenter and SRM servers.
 - DR site Active Directory services.
 - DR site DNS services.

- DR site VMware license services.
- The DR site has time synchronized to the same source or a source in sync with the primary site.
- All required NetApp volumes are being replicated using SnapMirror to the DR site.
- The SnapMirror operations have been monitored and are up to date with respect to the designed RPO.
- Required capacity exists on the DR NetApp controller. This refers to capacity required to support day-to-day operations that have been planned for in the DR environment.
- All DR ESX hosts already have iSCSI/FC sessions established with the DR storage arrays (physical arrays or vFilers) and appropriate igroups created.
- Some method exists to isolate the failed primary network from the DR site. This might be necessary if the event causing the disaster were temporary or intermittent in nature, such as an extended power outage. If power should be reapplied to the primary site, restarting systems and services might conflict with the recovered operations that are now running at the DR site.
- Plans have been made for providing users access to the applications and services at the DR site.

Note: It is important to make sure that a server performing the necessary Active Directory FSMO roles is available at the DR site. For information regarding transferring roles or seizing these roles, see Microsoft KB 255504 <http://support.microsoft.com/kb/255504>.

8.2 EXECUTING THE RECOVERY PLAN

A disaster has occurred that might require the environment to fail over to the DR site.

In this example, the two ESX hosts at the primary site, Site1, have been physically powered off. A connection to the vCenter server at the primary site shows the ESX hosts are not responding and the virtual machines hosted there indicate disconnected. For the purposes of this technical report, after verifying the ESX servers and virtual machines were no longer accessible, the primary vCenter server was also powered down to simulate a complete failure of Site1.

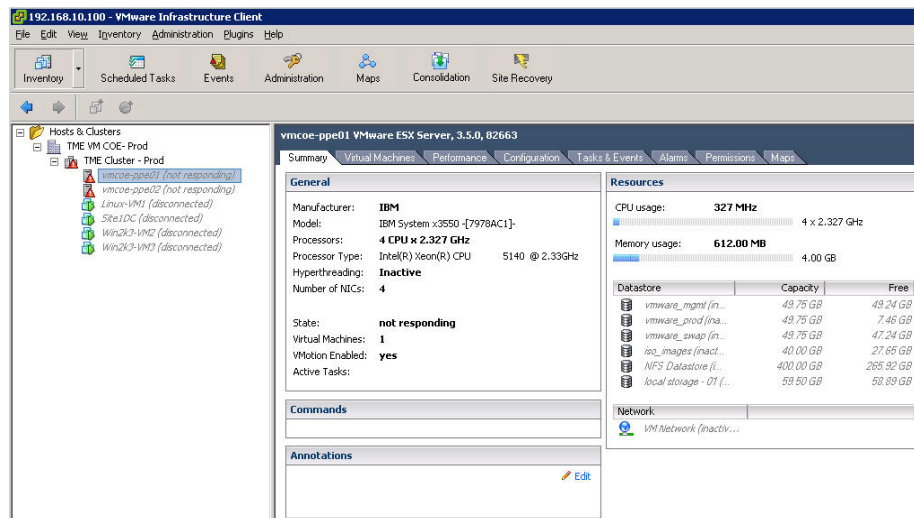


Figure 14 The ESX hosts and VMs at the primary site are down

As mentioned above the location of the placeholder VMs on the ESX hosts determines where they will startup. If not using DRS the ESX host used to start each VM in the recovery plan is the host on which the placeholder VM is currently registered. To help make sure that multiple VMs can be started simultaneously you should evenly distribute the placeholder VMs across ESX hosts before running the recovery plan. SRM will startup two VMs per ESX host, up to a maximum of 18 at a time, while executing the recovery plan. For more information about SRM VM startup performance see VMware vCenter Site Recovery Manager 4.0 Performance and Best Practices for Performance at www.vmware.com/files/pdf/VMware-vCenter-SRM-WP-EN.pdf

1. Before executing the DR plan, the administrative team must take predetermined steps to verify that a disaster has actually occurred and it is necessary to run the plan. After the disaster is confirmed, the team can continue with execution of the recovery plan.

2. Make a remote desktop connection to a system at the DR site. Launch the vSphere client and log into vCenter and select Site Recovery application. A login prompt appears to collect credentials for the primary vCenter server.
3. The connection fails due to the primary site disaster. The site recovery screen indicates that the paired site (in this case, the primary site) is "Not Responding" because that site is down.

Site Recovery for 192.168.10.101

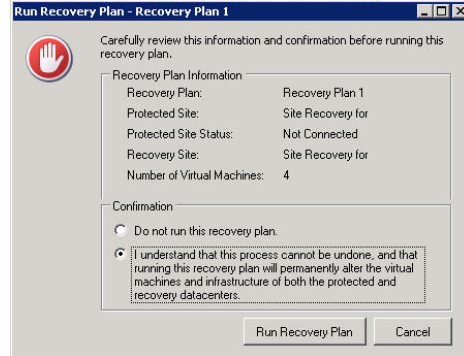
Local Site	Paired Site
VC Server: 192.168.10.101:443	VC Server: Not Responding
DR Server: 192.168.10.101:8095	DR Server: --
Site Name: Site Recovery for 192.168.10.101	Site Name: Site Recovery for 192.168.10.100

Setup

This server has not completed set up for disaster recovery. To complete configuration, follow the steps below.

Connection:	Not Connected	Configure Break
Array Managers:	Not Configured	Configure
Inventory Preferences:	Not Configured	Configure
Protection Groups:	0 Group(s) Created	Create
Recovery Plans:	1 Plan(s) Created	Create

4. From the tree on the left, select the recovery plan to be executed and click Run. Respond to the confirmation dialog and click Run Recovery Plan.



5. SRM runs the recovery plan. Note that the attempt to power down virtual machines at the primary site fails because they are inaccessible.
6. SRM breaks the SnapMirror relationship, making the DR site volumes writable, and mounts the datastores to the ESX hosts. The virtual machines are recovered and begin booting.

10.61.132.150 - Remote Desktop

192.168.10.101 - VMware Infrastructure Client

File Edit View Inventory Administration Plugins Help

Inventory Scheduled Tasks Events Administration Maps Consolidation Site Recovery

Hosts & Clusters

- SRM DR Site
 - DR Cluster
 - vmcoe-ppe03
 - vmcoe-ppe04
 - Linux-VM1
 - Site2DC
 - SRM DR VC Server
 - Win2K3-VM2
 - Win2K3-VM3

DR Cluster

Name	State	Status	Host	Host CPU - MHz	Host Mem - MB	Guest Mem - %	Not
Linux-VM1	Powered ...	○ ○ ●	vmcoe-ppe03	46	211	75	Not
SRM DR VC Server	Powered ...	○ ○ ●	vmcoe-ppe03	623	542	57	Not
Win2K3-VM2	Powered ...	○ ○ ●	vmcoe-ppe03	18	445	35	Not
Site2DC	Powered ...	○ ○ ●	vmcoe-ppe04	22	263	11	Not
Win2K3-VM3	Powered ...	○ ○ ●	vmcoe-ppe04	15	433	26	Not

SRM will mount NFS datastores during failover in the same way that it mounts datastores during DR testing, by alternating datastore mounts on IP addresses that were entered into the NFS IP Addresses field in the array setup dialog.

7. Connect to one of the virtual machines and verify access to the domain.
8. Continue on with whatever steps are necessary to complete a disaster recovery for business-critical applications and services.

9. If necessary and possible, isolate the primary site to prevent any conflicts if infrastructure services should be reestablished without warning.

9 RESYNC AFTER RECOVERY

9.1 REQUIREMENTS AND ASSUMPTIONS

After a disaster has been overcome, it is usually necessary to return operations back to the primary site. From a storage standpoint when considering the process of resyncing the environment back to the primary site there are three high-level scenarios to consider:

- A. Resyncing the environment if the primary storage has been recovered. This involves the use of the SnapMirror resync process, which requires that the primary and DR NetApp volumes have a common NetApp Snapshot copy that the SnapMirror software will recognize as a consistent point from which to resync.
- B. Resyncing the environment if the primary site storage was lost. In this case the primary storage might have been destroyed, or a common Snapshot copy no longer exists between the primary and DR volumes. This requires that the entire volume be initialized (a complete retransfer) back to the primary site using the SnapMirror initialize function.
- C. The third scenario is some combination of scenarios A and B, where loss of data might have occurred for some of the volumes at the primary site, but not all of them. In this case either a SnapMirror resync or SnapMirror initialize process would be done for each volume as appropriate.

The vSphere release of SRM provides no additional capability for automatic reversal and failback of storage replication or virtual machines.

DR failback requires the same processes as DR failover, with the primary difference being that it occurs at a preplanned time. To perform a proper, controlled failback, SRM should be used for failback by building protection groups and recovery plans in the reverse order.

This method of failback provides the following advantages over manual failback or scripted failback and brute force startup of virtual machines, all of which are as equally critical to a successful failback as they were to a successful failover:

- It's supported by VMware.
- Provides failback testing.
- Supports all storage protocols on all platforms.
- Provides virtual machine reconfiguration on failback, such as changes in IP addresses.
- Supports VMs using multiple datastores.
Note: VMFS datastores get resignatured by SRM on failover. To avoid broken links to virtual disks in multiple datastores VMs must be properly reconfigured by SRM on failback.
- Allows configuration of startup order of VMs so dependencies can be honored.

Resyncing after a disaster recovery requires the following processes:

1. Isolating the original environment prior to powering it on. This might be necessary to prevent outdated virtual machines from starting on the network, or any other conflicts with the DR environment that might occur (required only for scenario A).
2. Recovering and/or replacing the infrastructure at the primary site.
3. Reestablishing network connectivity between the sites.
4. Reversing the SnapMirror relationships (resync or initialize).
5. Building reverse SRM relationships.
6. Scheduling an outage to perform a controlled failover.
7. Running an SRM recovery plan in the opposite direction as was done in the disaster recovery.
8. Reestablishing normal operations. This involves reversing the SnapMirror and SRM relationships again to establish the original primary-to-DR site replication and protection.

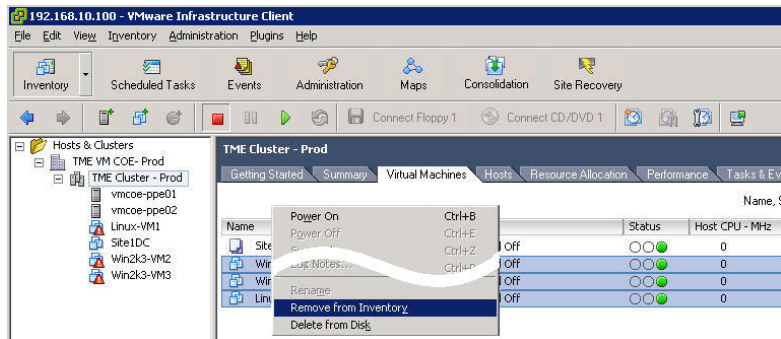
9.2 RESYNCING: PRIMARY STORAGE RECOVERED

Recovering back to an existing primary site, where an outage occurred but the primary array data was not lost is likely to be the most common scenario, so it is covered here first. If the disaster event that occurred did not cause the complete loss of data from the primary site, such as an unplanned power outage or planned failover, then SnapMirror allows replication of only the delta of new data back from the DR site. This enables very quick resync capability with minimized effect on the WAN link.

1. Recover the virtual infrastructure at the primary site. It is important in this scenario to make sure that the original ESX hosts do not begin to start outdated virtual machines on a network that might conflict with the DR site. There are a number of methods to prevent this, a simple one being to boot the storage appliances first and unmap LUNs from igroups to prevent virtual machines from being found and starting. Also consider disabling DRS and HA clustering services and any other systems in the primary environment that might require similar isolation.
2. Recover Active Directory and name resolution services at the primary site. This can be done by recovering the AD servers at that site and forcing them to resynchronize with the newer AD servers at the recovery site or by establishing new AD servers to synchronize.

Note: The AD servers at the original primary site that formerly serviced the FSMO roles that were seized must not be brought back online. Because those servers were down at the time the FSMO roles were seized, that server will be unaware that it is no longer responsible for providing those services. This server must be retired or re-commissioned as a new AD member server then promoted to a domain controller.

3. If the virtual machines at the primary site vCenter server still exist in inventory, they must be removed, or SRM will not be able to create the placeholder virtual machines when the reverse protection group is created.



4. After removing the old virtual machines from inventory, remove all LUNs or datastores from the ESX hosts at the primary site.
 - a. For iSCSI or FC datastores remove all LUNs of datastores to be failed back from the igroups on the NetApp arrays. After removing the LUNs from the igroups issue a storage rescan on each ESX host or cluster at the primary site.
 - b. For NFS datastores disconnect each datastore. In vSphere you can right click on a datastore and select Unmount. In the wizard that appears select every ESX host you wish to unmount the datastore.
5. When the VMs have been removed from inventory at the primary site and there is no risk of them coming online on the public network re-establish network connectivity between the sites to allow SnapMirror relationships to be established.
6. Reverse the SnapMirror relationships. The above steps above should be performed prior to reversing the SnapMirror relationships due to the fact that any datastores still connected to the ESX hosts will be made read-only by the resync, this could cause issues if done while the datastores are still connected. On the console of the primary site storage system, enter the `snapmirror resync` command to specify the DR site volume as the source with the `-S` switch.

```

vmcoe-fas3070-01> snapmirror resync -s DR site volume Primary site volume
vmcoe-fas2020-01:vmware_prod_dr vmcoe-fas3070-01:vmware_prod
The resync base snapshot will be: vmcoe-fas2020-01(0135018611)_vmware_prod_dr.13
Are you sure you want to resync the volume? y
Thu Apr 17 20:52:41 GMT [snapmirror.dst.resync.info:notice]: SnapMirror resync of vmware_prod to vmcoe-
fas2020-01:vmware_prod_dr is using vmcoe-fas2020-01(0135018611)_vmware_prod_dr.13 as the base snapshot.
Volume vmware_prod will be briefly unavailable before coming back online.
Thu Apr 17 20:52:42 GMT [waf1.snapstore.revert:notice]: Reverting volume vmware_prod to a previous sn
apshot.
Revert to resync base snapshot was successful.
Thu Apr 17 20:52:42 GMT [replication.dst.resync.success:notice]: SnapMirror resync of vmware_prod to vm
coe-fas2020-01:vmware_prod_dr was successful.
Transfer started.
Monitor progress with 'snapmirror status' or the snapmirror log.

```

For more information about the `snapmirror resync` command, see the Resynchronizing SnapMirror section of the *Data Protection Online Backup and Recovery Guide* for your version of Data ONTAP here: http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml.

7. Check the status of the transfer periodically until it is complete. Notice that the new DR-to-primary entry is now in the list of SnapMirror relationships along with the original primary-to-DR relationship. The primary-to-DR relationship is still recognized by the controllers, but no scheduled transfers would be permitted, as the DR volume has been made writable for use.

```

vmcoe-fas3070-01> snapmirror status
Snapmirror is on.

```

Source	Destination	State	Lag	Status
vmcoe-fas2020-01:vmware_prod_dr	vmcoe-fas3070-01:vmware_prod	Snapmirrored	03:11:12	Transfe
ring (117 MB done)				
vmcoe-fas3070-01:vmware_prod	vmcoe-fas2020-01:vmware_prod_dr	Source	03:11:12	Idle

8. Schedule SnapMirror updates to keep the relationship current until the failback is performed.
9. From the DR site vCenter server, configure the array manager for the protection side. In this case, the protection side is the DR site, and the recovery side is the original primary site. If you configured Array Managers with the arrays in opposite order as described earlier then you can simply proceed to the final screen of the wizard and click the Rescan Arrays button. If the reversed SnapMirror relationships are not detected on the first rescan verify the SnapMirror resync commands have completed and click the rescan button again.
10. Configure inventory preferences for the reverse SRM setup in the vSphere client at the DR site.
11. At the Primary site delete the original primary-to-DR protection groups. Because a real DR failover has been performed SRM will not allow these protection groups to be used again.
12. Create reverse protection groups at the DR site. Continue on through the protection group dialogs in the same manner as with the original configuration. A shared datastore will be required at the primary site for the placeholder virtual machines that SRM creates. If the primary site has a swapfile location, that may be used, or a small datastore created for this purpose.

Create Protection Group

Name and Description
Enter the name and description for new Protection Group

Name Virtual Machines Datastore Configure VMs	Protection group name: Failback Protection Group 1 Description:
---	---

13. Create reverse recovery plans at the primary site. Work through the Recovery Plan wizard in the same way as in the original setup procedure. Note that a test network providing connectivity between ESX

hosts may be required for DR testing just as with the original failover setup.

Create New Recovery Plan

Recovery Plan Information
Enter the name and description for this recovery plan.

Recovery Plan Information

- Protection Groups
- Response Times
- Networks
- Virtual Machines to Suspend

Name: Failback Recovery Plan 1

Description:

14. Verify that the SnapMirror relationship has completed transferring and that it is up to date.
15. Perform a SnapMirror update if necessary and perform a test run of the recovery plan.
16. When the recovery plans and other necessary infrastructure have been established at the primary site, schedule an outage to perform a controlled failover.
17. When appropriate, notify the users of the outage and begin executing the failback plan.
18. During the scheduled failback, if allowed to do so, SRM will shut down the virtual machines at the DR site when the recovery plan is executed. However, this is not desired in most cases. Instead of allowing SRM to shut down the virtual machines, perform a controlled proper shutdown of application and infrastructure virtual machines at the DR site. This helps make sure that all applications are stopped, users are disconnected, and no changes are being made to data that would not get replicated back to the primary site.
19. Once the environment to be failed back is properly shut down, perform a final SnapMirror update to transfer any remaining data back to the primary site.

```
vmcoe-fas3070-01> snapmirror update -S vmcoe-fas2020-01:vmware_prod_dr vmcoe-fas3070-01:vmware_prod
Transfer started.
Monitor progress with 'snapmirror status' or the snapmirror log.

vmcoe-fas3070-01> snapmirror status
Snapmirror is on.
Source Destination State Lag Status
vmcoe-fas2020-01:vmware_prod_dr vmcoe-fas3070-01:vmware_prod Snapmirrored - Idle
vmcoe-fas3070-01:vmware_prod vmcoe-fas2020-01:vmware_prod_dr Source 03:48:13 Idle
```

20. Execute an SRM recovery plan in the opposite direction as was done in the disaster recovery.

192.168.10.100 - VMware Infrastructure Client

File Edit View Inventory Administration Plugins Help

Run Recovery Plan - Failback Recovery Plan 1

Carefully review this information and confirmation before running this recovery plan.

Recovery Plan Information

- Recovery Plan: Failback Recovery Plan 1
- Protected Site: Site Recovery for
- Protected Site Status: Connected
- Recovery Site: Site Recovery for
- Number of Virtual Machines: 4

Confirmation

☐ Do not run this recovery plan.

☒ I understand that this process cannot be undone, and that running this recovery plan will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Run Recovery Plan Cancel

3. Power off VM "Win2k3-VM2"

2. Shutdown Primary Site VM "Win2k3-VM1"

1. Shutdown Guest OS for Remote Site

21. Verify the recovered environment and allow users to connect and continue normal business operations.
22. Reestablish primary-to-DR replication.

9.3 RESYNCING: PRIMARY STORAGE LOST

In this case the outage that was cause for the failover of the environment to the DR site was such that it caused the complete loss of data from the primary storage or the complete loss of the infrastructure at the primary site. From a SnapMirror and SRM point of view, recovery from such an event is nearly identical to the steps in the section above. An exception is that once the infrastructure at the primary site has been recovered or replaced, a SnapMirror initialize action must be performed to replicate the entire content of required data back from the DR site to the primary.

All of the steps necessary for recovery are not reiterated in detail here. It is important to note that if the WAN link between the sites is sufficient to allow the complete transfer of data over the WAN, then this process would be nearly identical to the process documented above with the exception that, once the primary storage had been replaced and made available, the “snapmirror initialize -S <dr_controller>:<dr_volume> <primary_controller>:<primary_volume>” command would be used in place of the “snapmirror resync -S” command in the section above.

If a complete transfer of data over the WAN to the primary site is not possible, consult the SnapMirror Best Practices Guide for information regarding other methods of a SnapMirror initialization, including SnapMirror to tape, or cascading SnapMirror through an intermediate system:

www.netapp.com/us/library/technical-reports/tr-3446.html.

1. Recover or replace the infrastructure at the primary site as necessary, including but not limited to:
 - a. The VMware vCenter server, including the installation and configuration of the SRM plug-in
 - b. The VMware ESX hosts and any custom settings that were previously configured, time synchronization, admin access, and so on
 - c. The NetApp primary storage, including volumes that data from the DR site will be recovered into
 - d. The igroups necessary for the ESX hosts to connect
 - e. The network infrastructure necessary
2. Configure network connectivity between the sites to allow SnapMirror relationships to be established.
3. Initialize the SnapMirror relationships. On the console of the primary site storage system the SnapMirror initialize command is used specifying the DR site volume as the source with the -S switch.
4. Check the status of the transfer periodically until it is complete.
5. At this time create SnapMirror schedule entries to keep the relationship up to date until the failback is scheduled.
6. Build reverse SRM relationships.
7. From the DR site vCenter server configure the array manager for the protection side.
8. Configure the recovery-side array manager.
9. Configure inventory preferences for the reverse SRM setup.
10. Create reverse protection groups at the DR site.
11. Create reverse recovery plans at the primary site.
12. Verify that the SnapMirror relationship has completed transferring and that it is up to date.
13. Perform a SnapMirror update if necessary and perform a test run of the recovery plan.
14. If all is well with the recovery plan and the other necessary infrastructure at the primary site, schedule an outage to perform a controlled failover.
15. When appropriate, notify the users of the outage and begin executing the failback plan.
16. During the scheduled failover, if allowed to do so, SRM will shut down the virtual machines at the DR site when the recovery plan is executed. However, this is not desired in most cases. Instead of allowing SRM to shut down the virtual machines, perform a controlled proper shutdown of application and infrastructure virtual machines at the DR site. This helps make sure that all applications are stopped, users are disconnected, and no changes are being made to data that would not get replicated back to the primary site.
17. Once the environment to be failed back is properly shut down, perform a final SnapMirror update to transfer any remaining data back to the primary site.

18. Execute an SRM recovery plan in the opposite direction as was done in the disaster recovery.
19. Verify the recovered environment and allow users to connect and continue normal business operations.
20. Reestablish primary-to-DR replication.

9.4 REESTABLISHING PRIMARY-TO-DR REPLICATION

Reestablishing normal operations requires the following processes:

1. Reversing the SnapMirror and SRM relationships again, to establish the original primary-to-DR site replication and protection.
For more information, see the *Resynchronizing SnapMirror* section of the *Data Protection Online Backup and Recovery Guide* for your version of Data ONTAP for instructions:
http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml.
2. Clean up all remaining unnecessary SnapMirror relationships using the SnapMirror release command and by deleting Snapshot copies that were created for the temporary SnapMirror relationships as necessary.
For more information, see the *Releasing Partners from a SnapMirror Relationship* section of the *Data Protection Online Backup and Recovery Guide* for your version of Data ONTAP for instructions:
http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml.
3. Rebuild the original SRM protection groups and recovery plans.

Note: If the test button does not appear active after establishing protection for a virtual machine, verify that there were no preexisting shadow virtual machine directories in the temporary datastore at the DR site. If these directories exist, it might be necessary to delete and recreate the protection group for those VMs. If these directories remain, they might prevent the ability to run a DR test or failover.

10 BEST PRACTICES

ENSURING THE QUICKEST STARTUP AT THE DR SITE

The ESX host used to start each VM in the recovery plan is the host on which the placeholder VM is currently registered. To help make sure that multiple VMs can be started simultaneously you should spread the placeholder VMs across ESX hosts before running the recovery plan. Make sure that in each step of the recovery plan, for example high priority and normal priority, the VMs are separated onto different ESX hosts. SRM will startup two VMs per ESX host while executing the recovery plan. For more information about SRM VM startup performance see VMware vCenter Site Recovery Manager 4.0 Performance and Best Practices for Performance at www.vmware.com/files/pdf/VMware-vCenter-SRM-WP-EN.pdf

NETAPP VOLUMES AND SRM PROTECTION GROUPS

Volume-based SnapMirror works by replicating Snapshot copies at the volume level. Because of this NetApp volumes, or groups of volumes, work well as the basis for protection groups. If the data layout was done according to the designs described in TR-3428, then NetApp volumes should map nicely to VMware protection groups.

NETWORK FOR DR TESTING

Create a physical test bubble network by segregating a physical network or a VLAN to link the ESX test bubble networks. A possible cost-free solution to consider is to use the physical infrastructure of the VMotion® network at the DR site. VMware best practices recommend a separate VMotion network. If the DR VMotion network is not utilized outside of DR activities or during DR testing and is already segregated from the public network, then adding a test bubble network to the VMotion vSwitch can provide this infrastructure. Make sure that this network is segregated using VLANs or VLAN tagging to isolate the IP addresses of the DR virtual machines as they are recovered.

VIRTUAL MACHINE STARTUP DEPENDENCIES

In the protection group, set important infrastructure servers at high priority to make sure they are recovered first. Also consider inserting a message step into the recovery plan after the step that recovers the high-priority virtual machines. This will pause the execution of the recovery plan at this point. During a DR test or true DR scenario verify the infrastructure services are available before other servers with dependencies are recovered.

Another option, with regard to infrastructure server dependencies, is to put such servers in a protection group to be recovered and verified first, before application server protection groups are recovered.

Make sure that each protection group/recovery plan contains the appropriate infrastructure servers, such as Active Directory servers, to facilitate testing in the DR test bubble networks.

PROVIDING ACTIVE DIRECTORY SERVICES AT THE DR SITE

It is recommended that Microsoft Active Directory servers not be recovered with SRM as this can result in issues with domain controllers becoming out of sync in the environment. Active Directory services can be more reliably provided at the DR site by using existing servers in that location.

DOCUMENTATION AND MESSAGE STEPS

Document any specifics of the DR plan that are not maintained specifically within SRM. For example, if you have built multiple recovery plans that must be ran in a specific order or only after other external requirements have been met ensure these are documented and use the message step feature, inserting a message step at the beginning of the outlining any external requirements for a successful run of that plan.

REALISTIC DR TESTING

Perform a realistic walk-through test. Don't depend on any infrastructure or services that won't be available during a real DR scenario. For example, make sure you are not relying on primary site name resolution services while performing a DR test.

Using the test bubble network to verify application server operation is part of a complete test.

11 KNOWN BEHAVIORS

SRM DOES NOT INVOKE/CONFIGURE SNAPMIRROR TRANSFERS

SRM will only invoke SnapMirror quiesce and break commands. SnapMirror configuration and update scheduling must be done outside of SRM and prior to configuring SRM. For best practices on configuring your SnapMirror transfers, see the SnapMirror Best Practices Guide, TR-3446.

MANAGING RDM DEVICES WITH NETAPP SNAPDRIVE FOR WINDOWS

NetApp SnapDrive for Windows manages the creation of snapshots for LUNs connected to VMs by raw device maps. To do this SnapDrive requires access to the vCenter server managing the VM. After a SRM failover the vCenter server has been changed to the server at the DR site. For SnapDrive to function properly after failover the vCenter server setting must be updated. This can be automated using SRM command steps. For details please see NetApp KB article [kb56952](https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb56952)
<https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb56952>

SUPPORTED SNAPMIRROR VOLUME LAYOUTS

Be sure to follow the data layout rules outlined in the section Requirements and Assumptions above to make sure of supportability with SRM.

RDM SUPPORT

With the release of VMware vCenter Site Recovery Manager version 1.0U1 raw disk maps are now supported in SRM.

SRM DYNAMIC LUN ACCESS

Compute resources (ESX hosts and clusters) are mapped between sites in SRM inventory mappings. ESX clusters or individual non-clustered ESX hosts can be mapped to ESX clusters or non-clustered ESX hosts at the DR site. When individual ESX hosts are mapped between sites SRM will attempt to recovery LUNs and present the recovered LUNs only to the specific ESX host as specified in the inventory mappings settings, this is referred to as dynamic LUN access in SRM.

If you have followed NetApp best practices in TR-3428 for VI3 or TR-3749 for vSphere where it is recommended to create one igroup for each cluster or group of ESX hosts that share LUNs, then it may not be possible for the storage adapter to present a LUN only to one specific ESX host. Instead the LUN will be presented in the single igroup and be made visible to all ESX hosts in that igroup. This is typically acceptable as implementing the cluster igroup model indicates that the intended design was that all LUNs presented to a host in the cluster or igroup should be accessible by any host in that cluster. However, if it is required that a LUN recovered by SRM be presented to only one host or subset of hosts at the DR site then

it is necessary to configure the environment with an igroup for each ESX host, rather than creating one igroup for the entire cluster or group of hosts.

STORAGE RESCANS

In some cases ESX might require a second storage rescan before a newly connected datastore is recognized. In this case the SRM recovery plan might fail, indicating that a storage location cannot be found even though the storage has been properly prepared during the DR test or failover.

For VI3 environments a workaround is provided in the VMware SRM release notes here:

http://www.vmware.com/support/srm/srm_10_releasenotes.html - miscellaneous.

In vSphere environments the same workaround can be applied in the GUI by right-clicking the Site Recovery icon in the upper left of the SRM GUI, selecting Advanced Settings, and adjusting the SanProvider.hostRescanRepeatCnt value.

PREFIX ON DATASTORE NAMES

By default VMFS datastores that are recovered by SRM during a DR test or failover will be prefixed with a character string snap-xxxxx. This is standard behavior when a clone of a previously connected datastore is attached to an ESX server.

In VI3 environments can be configured to maintain datastore names by making the following change in the SRM xml configuration file at C:\Program Files\VMware\VMware Site Recovery Manager\config\vmware-dr.xml on the recovery-side SRM server.

Change the line:

```
<fixRecoveredDatastoreNames>false</fixRecoveredDatastoreNames>
```

To read:

```
<fixRecoveredDatastoreNames>true</fixRecoveredDatastoreNames>
```

In vSphere environments right-clicking the Site Recovery icon in the upper left of the SRM GUI, selecting Advanced Settings, and adjusting the SanProvider.fixRecoveredDatastoreNames value can control this behavior.

FIREWALL RULES: TCP PORTS

To enable communication in an SRM environment the following ports must be available.

SRM server to vCenter server (local site only):

- SOAP port 8095 (default)
- SRM Client Download HTTP port 8096 (default)
- SRM External API SOAP port 9007 (default)

SRM communication (site-to-site):

- HTTP port 80

Note: SRM creates tunnel to the vCenter server on port 80, then performs an SSL handshake within that tunnel. (It does not use port 443.)

SRM to storage communication (local and site-to-site):

- HTTP port 80 (default)
- SSL port 443 (if SecureAdmin™ software is configured in Data ONTAP)

Additional steps are required to enable SSL communication between a SRM storage adapter and storage array. Please see the following kb article for more information

<https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb54012>

LOG FILES

Log files for SRM are stored in the following location on each SRM server:

C:\Documents and Settings\All Users\Application Data\VMware\VMware Site Recovery Manager\Logs Note that commands sent to remote site arrays are sent by proxy through the remote SRM server, so checking logs at both sites is important when troubleshooting.

CLEANING UP SHADOW VMS (DR TEST BUTTON DISABLED)

If the test button does not appear active after establishing protection for a virtual machine, verify that there were no preexisting shadow virtual machine directories in the temporary datastore at the DR site. If these

directories exist, it might be necessary to delete and recreate the protection group for those VMs. If these directories remain, they might prevent the ability to run a DR test or failover.

NFS SUPPORT

NFS support requires SRM 4.0 and vCenter 4.0. ESX 3.0.3, ESX/ESXi 3.5U3+ and 4.0 are also supported for SRM with NFS.

USING THE RW (READ/WRITE) FIELD IN NFS EXPORTS

NFS support requires that replicated NFS datastores exported from the NetApp array using values in the RW field. An NFS export with a default RW field value of empty, meaning export RW to all hosts, will not be discovered by the NAS adapter.

SRM ARRAYS ARE NETAPP CONTROLLERS

Each controller in a NetApp HA cluster takeover pair is considered an array in SRM. Each controller must be added to array managers separately. In environments using both the SAN and NAS adapters, each controller must be added both as a SAN array and as a NAS array.

ROLE-BASED ACCESS CONTROLS FOR THE STORAGE ADAPTERS

Instructions and rights required to configure Data ONTAP role-based access controls for the accounts used as array credentials with SRM 4 can be found in KB article [1010829](https://kb.netapp.com/support/index?page=content&id=1010829) at <https://kb.netapp.com/support/index?page=content&id=1010829>.

Instructions and rights required to configure Data ONTAP role-based access controls for the accounts used as array credentials with SRM 5 can be found in KB article [1013325](https://kb.netapp.com/support/index?page=content&id=1013325) at <https://kb.netapp.com/support/index?page=content&id=1013325>.

SETTING WORKINGDIR VARIABLE IN VMX FILE AFFECTS SRM RECOVERABILITY

Setting a custom value for the workingDir variable in a .vmx file changes the location where ESX stores virtual machine Snapshot delta files. SRM does not support storing Snapshot delta files outside of replicated datastores. See the appendix regarding protecting virtual machines without replicating transient data.

DEPLOYING DIFFERENT STORAGE PROTOCOLS AT PRIMARY AND DR SITES

SRM and Data ONTAP do support having differing SAN storage protocols at the primary and DR sites. For example, you can use a lower cost software iSCSI solution at the DR site while the primary site is using Fibre Channel. However, NFS cannot be used to recover SAN storage, and SAN protocols cannot be used to recover NFS storage.

APPLICATION CONSISTENCY

SRM and SnapMirror do not provide application consistency. Application consistency is determined by the consistency level stored in the image of data that is replicated. If application consistent recovery is desired applications such as Microsoft SQL Server®, Microsoft Exchange Server® or Microsoft Office SharePoint Server must be made consistent using software such as the NetApp SnapManager® products. Implementation of SRM in an environment with virtual machines running SQL, Exchange and SharePoint is described in detail in TR-3822 Disaster Recovery of Microsoft Exchange, SQL Server, and SharePoint Server using VMware vCenter Site Recovery Manager, NetApp SnapManager and SnapMirror, and Cisco Nexus Unified Fabric.

12 REFERENCE MATERIALS

[TR-3749: NetApp and VMware vSphere Storage Best Practices](https://www.netapp.com/us/library/technical-reports/tr-3749.html)

www.netapp.com/us/library/technical-reports/tr-3749.html

[TR-3428: NetApp and VMware Virtual Infrastructure 3 Storage Best Practices](https://www.netapp.com/us/library/technical-reports/tr-3428.html)

www.netapp.com/us/library/technical-reports/tr-3428.html

[TR-3446: SnapMirror Best Practices Guide](https://www.netapp.com/us/library/technical-reports/tr-3446.html)

www.netapp.com/us/library/technical-reports/tr-3446.html

[TR-3822: Disaster Recovery of Microsoft Exchange, SQL Server, and SharePoint Server using VMware vCenter Site Recovery Manager, NetApp SnapManager and SnapMirror, and Cisco Nexus Unified Fabric](https://www.netapp.com/us/library/technical-reports/tr-3822.html)

www.netapp.com/us/library/technical-reports/tr-3822.html

[VMware vCenter Site Recovery Manager 4.0 Performance and Best Practices for Performance
www.vmware.com/files/pdf/VMware-vCenter-SRM-WP-EN.pdf](http://www.vmware.com/files/pdf/VMware-vCenter-SRM-WP-EN.pdf)

SRM System Administration guides and Release notes from the [VMware vCenter Site Recovery Manager
Documentation](http://www.vmware.com/support/pubs/srm_pubs.html) site www.vmware.com/support/pubs/srm_pubs.html

APPENDIX A: VMS WITH NONREPLICATED TRANSIENT DATA

If the transient data in your environment, such as VMware virtual machine swapfiles or Windows system pagefiles, has been separated onto nonreplicated datastores, then ESX and SRM might be configured to recover virtual machines while maintaining the separation of that data.

Below is an image describing the environment represented in this document, with the addition that transient data contained in Windows pagefiles and VMware *.vswp files has been separated into a nonreplicated datastore.

At both the primary and DR sites nonreplicated volumes have been created to contain ESX datastores for virtual machine swapfiles and pagefiles. See below for information regarding configuring the systems to use these datastores for transient data storage.

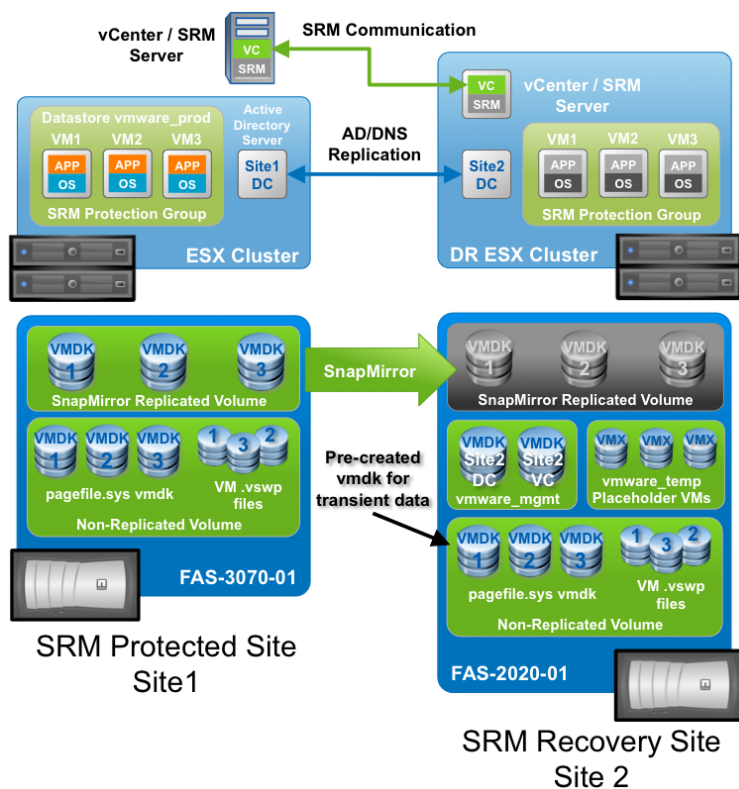


Figure 15 SRM with Non-Replicated Transient Data

PROTECTING VMS ON ESX HOSTS WITH NONREPLICATED SWAPFILES

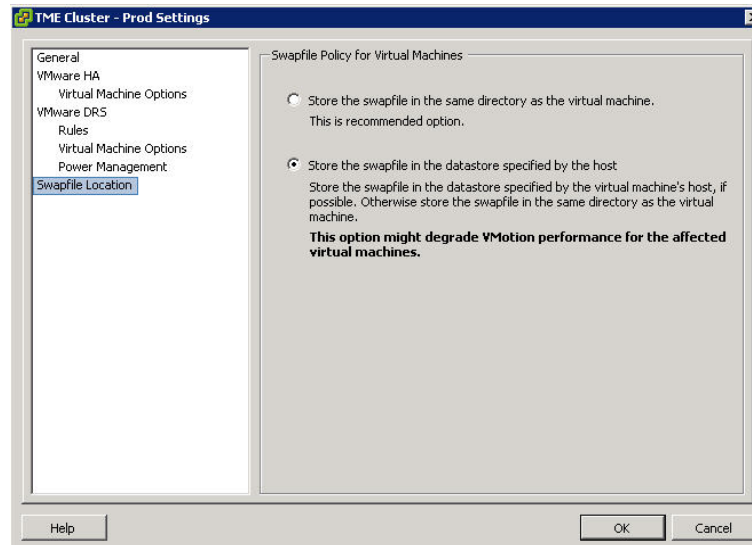
When a virtual machine is powered on, a virtual swapfile is created on disk equal to the size of the memory allocated in the virtual machine. For example, when the virtual machine Win2k3-VM2 is powered on, a file called Win2k3-VM2-0c657624.vswp is created in the configured location.

By default this vswp file is stored in the same location as the virtual machine, causing this data to be replicated, along with the configuration files for the virtual machine and its virtual disk file. The location of the vswp file can be changed with the following procedures.

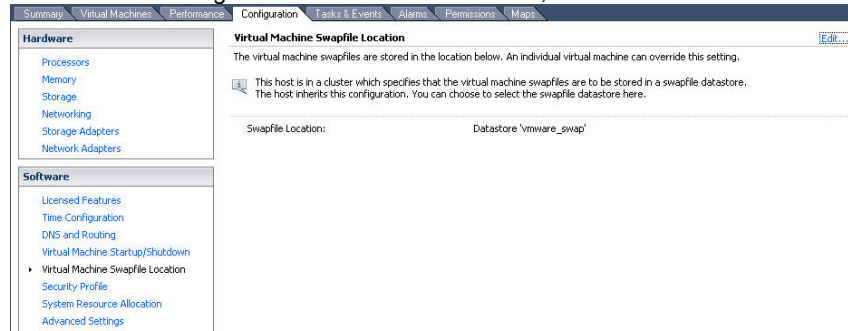
CONFIGURING THE VSWAP FILE LOCATION IN ESX 3.5 AND 4.0

In ESX 3.5 configure the ESX cluster settings to use the location specified by the ESX hosts to store swapfiles. Then, on each ESX host specify the name of a nonreplicated datastore for swapfiles.

1. In the vCenter server at the primary site right-click the ESX cluster and select Edit Settings. Click Swapfile Location and choose the option "Store the swapfile in the datastore specified by the host." Click OK.



2. In the vCenter configuration tab for each ESX host, click the Virtual Machine Swapfile Location link.



3. Click the Edit... link and select a shared datastore for this cluster that is located in the primary site.
4. At the DR site configure the ESX clusters and hosts in the same manner, this time selecting a shared datastore for swapfiles that is located in the DR site.

As virtual machines are recovered by SRM at the DR site, the swapfiles will be created in the selected datastore. There is no need for the transient vmswap file data to be replicated to the DR site.

CONFIGURING THE VSWAP FILE LOCATION IN ESX 3.0.2

The vswap file location can be specified in ESX 3.0.2 virtual machines by configuring options in the vmx configuration files.

1. Properly shut down the virtual machine to be modified and make a backup copy of its vmx file.
2. Edit the vmx file making the following changes.

- a. `sched.swap.dir = "/vmfs/volumes/vmware_swap"`

Set the sched.swap.dir value to the location of the shared swapfile datastore at the DR site.

Note: Setting the swapfile location explicitly in the vmx file requires that the swapfile datastore at the DR site have the exact same name as the swapfile datastore specified in the vmx file.

Otherwise, when the virtual machine is recovered by SRM at the DR site, it will not be able to locate the datastore and will not power on.

- b. `sched.swap.derivedName = "/vmfs/volumes/47f4bec7-ad4ad36e-b80a-001a64115cba/Linux-VM1-f18ee835.vswp"`

Delete the sched.swap.derivedName option. This line will be automatically recreated by ESX when the virtual machine is powered on. It is set to the physical path name of the vswp file location.

- c. workingDir = "."

This is the default setting for this option. Leave this setting as is. Changing the workingDir variable moves the location of VMware Snapshot delta files, which is not supported by SRM, as SRM requires that Snapshot delta files be on replicated datastores due to the fact that these files contain virtual machine data.

3. Save the vmx file and power on the virtual machine.
4. Browse the vmware_swap datastore and verify a new vswp file was created there when the virtual machine powered on.
5. Make sure there is a nonreplicated datastore at the DR site also named vmware_swap with adequate capacity to contain the vswp files.

PROTECTING VMS WITH NONREPLICATED WINDOWS PAGE FILES

By default Windows hosts store the virtual memory pagefile on the system drive, but they can be configured to store the pagefile on a second virtual disk. This virtual disk can be stored in a nonreplicated datastore; however, to prevent Windows from placing the pagefile back in the default location when it's recovered at the DR site, steps must be taken to provide a virtual disk for the pagefile to be placed there.

If the pagefile does get placed back on the system disk, then that amount of capacity must be resynced back to the primary site, or extra downtime for the virtual machines and complicated administrative work would be required to remove the pagefile from the system drive prior to resyncing the environments.

SRM can be configured to connect a preexisting vm disk to a recovered virtual machine at the DR site. To make sure that this disk is recognized by the Windows virtual machine as the same disk where the pagefile was stored at the primary site, the pre-created disk must have the same disk signature as the disk at the primary site. VMware disk cloning can be used in a procedure to accomplish this.

The process below is an example of configuring Windows virtual machines and SRM to utilize nonreplicated storage for Windows pagefiles.

1. At the primary site edit a temporary Windows virtual machine configuration. Create a virtual disk and store this disk in a location where virtual machine templates would typically be stored: for example, /vmfs/volumes/templates/pagefile_disks/pagefile.vmdk. This virtual disk will serve as the basis for all other pagefile virtual disks to be cloned from.
2. In the virtual machine, enter Disk Management, rescan for storage, and allow Windows to write a signature on the disk. Create a partition on the disk and format it.
3. Disconnect the Windows host from the disk.
4. Create a clone of the virtual disk for each Windows virtual machine by using the `vmkfstools` command. Store these virtual machines in a nonreplicated datastore such as vmware_swap. In this example, a clone is created for Win2k3-VM2, and the clone is stored in a directory for that virtual machine.

```
[root@vmcoe-ppe01 vmware_swap]# mkdir /vmfs/volumes/vmware_swap/vm2_pagefile
```

```
[root@vmcoe-ppe01 vmware_swap]# vmkfstools -i  
/vmfs/volumes/templates/pagefile_disks/pagefile.vmdk  
/vmfs/volumes/vmware_swap/vm2_pagefile/pagefile.vmdk
```

5. In vCenter, connect each pagefile.vmdk to the appropriate virtual machine.
6. Connect to each virtual machine console, open Disk Management, and rescan for storage. Assign a drive letter to the disk; in this process P: is assigned.
7. Configure each Windows virtual machine to use P: for its virtual memory location. The change requires a reboot. After Windows has stopped using the system drive for virtual memory, the pagefile.sys file might be deleted from the system disk. An example of a regedit file with the appropriate keys to

configure the location of the Windows pagefile, as well as some other miscellaneous temporary data, can be found in TR-3428: NetApp and VMware Virtual Infrastructure 3 Storage Best Practices.

8. Copy the original pagefile vmdk, /vmfs/volumes/templates/pagefile_disks/pagefile.vmdk, to the DR site. This can be done using cp across a NAS share, FTP, and so on. Be sure to copy both the pagefile.vmdk and pagefile-flat.vmdk files.
9. Using the disk just copied to the DR site as the source, create clones in the swapfile datastore at the DR site for each virtual machine to connect to as they are recovered there by SRM.

```
[root@vmcoe-ppe03 vmware_swap_dr]# mkdir /vmfs/volumes/vmware_swap_dr/vm2_pagefile
```

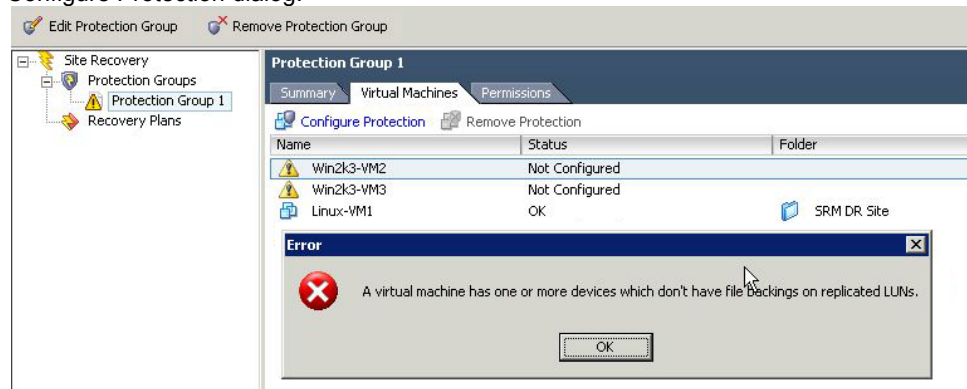
```
[root@vmcoe-ppe03 vmware_swap]# vmkfstools -i  
/vmfs/volumes/dr_templates/pagefile_disks/pagefile.vmdk  
/vmfs/volumes/vmware_swap_dr/vm2_pagefile/pagefile.vmdk
```

The clone preserves the disk signature of the vmdk. Each Windows host has been connected to a disk with this signature as the P: drive at the primary site. If SRM is configured to attach this cloned disk to each virtual machine as it is recovered, then Windows will recognize the disk as its P: drive and configure its pagefile there upon booting.

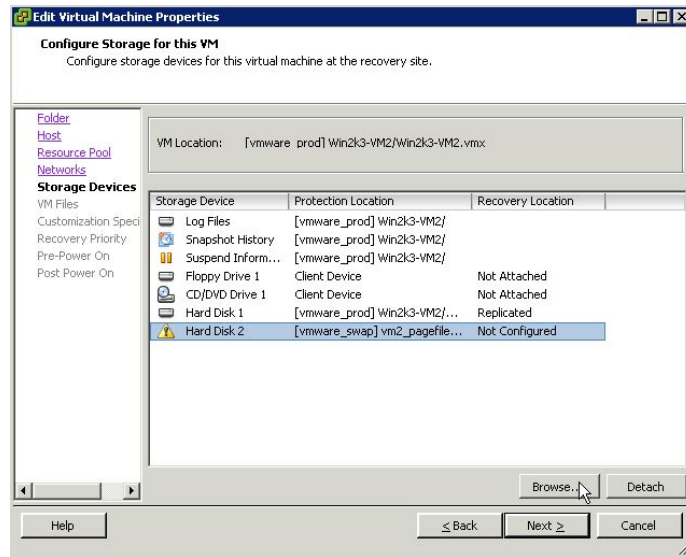
10. In the vCenter server at the primary site display the protection group. Click the Virtual Machines tab. When a virtual machine has a virtual disk stored on nonreplicated storage, SRM will recognize this virtual disk and display a warning on the virtual machine. Select a virtual machine and click the Configure Protection link.



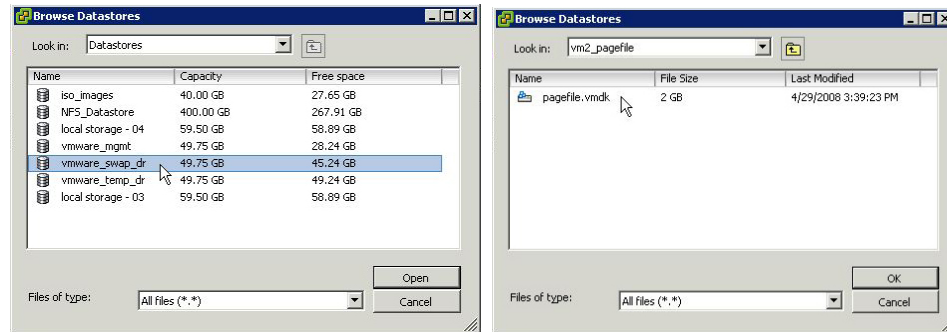
11. A warning about the problem with the virtual machine will be displayed. Click OK and continue to the Configure Protection dialog.



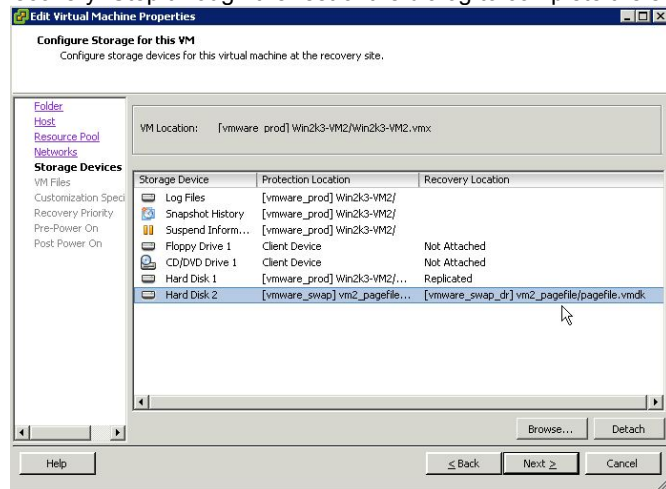
12. Proceed to the Storage Devices step. Select the virtual disk where the pagefile is stored. Click Browse.



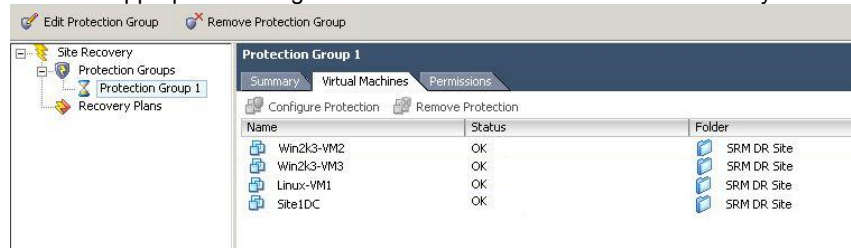
13. Select the datastore where this virtual machines DR pagefile disk is stored, select the vmdk, and click OK.



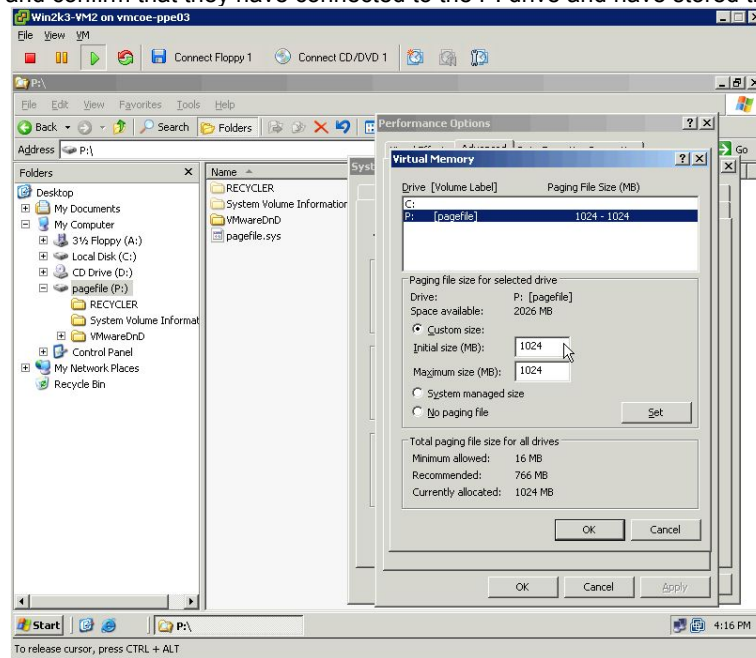
14. Confirm that the Storage Devices screen indicates the proper location for the disk to be attached on recovery. Step through the rest of the dialog to complete the settings.



15. Make the appropriate changes for each of the virtual machines until they are all configured properly.



16. Click the Summary tab and confirm the protection group status is OK, indicating it has synced with the DR site.
17. Perform a SnapMirror update, if necessary, to make sure that the virtual machines and their configuration files have been replicated to the DR site.
18. In vCenter at the DR site run a test of the recovery plan. Connect to the console of the virtual machines and confirm that they have connected to the P: drive and have stored the pagefile there.



APPENDIX B: NON-QUIESCED SMVI SNAPSHOT RECOVERY

By default the NetApp adapter recovers FlexVol volumes to the last replication point transferred by NetApp SnapMirror. The 1.4.3 release of the NetApp SRM adapter provides the capability to recover NetApp volume snapshots created by NetApp SnapManager for Virtual Infrastructure. This feature is not available in NetApp FAS/V-Series Storage Replication Adapter 2.0 for SRM 5.

This functionality is currently limited to support for snapshots created without using the option to create a VMware consistency snapshot when the SMVI backup is created. Considering that by default the adapter recovers the same type of image as that created by a non-quieted SMVI created snapshot, this feature currently has limited use cases. An example use case for this functionality would be that an application requires recovery to the specific point in time that was created by the SMVI backup. For example, an application runs in a VM that cannot be recovered unless it is recovered from a specific state. A custom script is used with SMVI to place the application into this state and during this state the SMVI backup is performed creating the NetApp Snapshot. The NetApp Snapshot now recovered by the adapter will contain the VM with the application in the required state.

NON-QUIESCED SMVI SNAPSHOT RECOVERY CONFIGURATION RULES

The following configuration limitations apply when using the option to recover non-quieted SMVI snapshots with the NetApp adapter:

- This feature requires SMVI version 2.0 or newer.
- Only recovery to the most recently created SMVI snapshot is allowed.
- The option to create a VMware consistency snapshot when the SMVI backup is created must be disabled for the SMVI job that creates the backup used for this purpose. (The NetApp adapter will determine if this option was disabled before allowing use of the snapshot.)
- The option is only supported with volume level Asynchronous SnapMirror.
- There should be only one VMware datastore in each NetApp FlexVol being recovered.
- A SnapRestore license is required on the NetApp system.
- This is a global option that is set for all recovery plans executed while the option is set. To enable it for specific recovery plans the option must be changed before running the desired plan.

USING THE NON-QUIESCED SMVI SNAPSHOT RECOVER FEATURE

To enable the feature change the `use_smvi_snapshot` option in the `ontap_config.txt` file located by default on the recovery site SRM server at `C:\Program Files\VMware\VMware vCenter Site Recovery Manager\scripts\SAN\ONTAP\ontap_config.txt`.

Setting the value of `use_smvi_snapshot` to off enables the default behavior of the adapter to recover all NetApp FlexVol volumes to the replication point created by SnapMirror.

Setting the value of `use_smvi_snapshot` to on enables non-quieted SMVI snapshot recovery.

The behavior of the NetApp adapter with the option enabled depends on the recovery mode SRM is currently executing.

DR test mode – A FlexClone volume is created using the most recent non-quieted SMVI created NetApp snapshot as the base snapshot of the clone. If any SMVI created snapshots newer than the most recent non-quieted SMVI created snapshots exist on the volume then the adapter will fail to recover the datastore and report this failure to SRM.

DR failover mode – The FlexVol volume is reverted to the most recent SMVI created NetApp snapshot. If any SMVI created snapshots newer than the most recent non-quieted SMVI created snapshots exist on the volume then the adapter will fail to recover the datastore and report this failure to SRM. To proceed with recovery in this case, the administrator may remove the newer snapshots from the FlexVol volume and re-run the recovery plan. SRM will re-attempt any failed storage recovery steps from the previous run. Alternatively the administrator may disable the `use_smvi_snapshot` option restoring the default behavior and re-run the recovery plan.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication or with respect to any results that might be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein must be used solely in connection with the NetApp products discussed in this document.

© Copyright 2012 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, Data ONTAP, FlexClone, FlexVol, NearStore, SnapDrive, SnapManager, SnapMirror, SnapRestore, and Snapshot are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Microsoft, SharePoint, SQL Server, and Windows are registered trademarks of Microsoft Corporation. VMware is a registered trademark and vCenter, VMotion, and vSphere are trademarks of VMware, Inc. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

